

INFOWATCH

InfoWatch Traffic Monitor 6.1

Руководство пользователя

InfoWatch Traffic Monitor 6.1

Руководство пользователя

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

Дата редакции: 2016-10-24

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 7

1.1 Аудитория 7
1.2 Комплект документов 7
1.3 Техническая поддержка пользователей 7

2 ОБЗОР INFOWATCH TRAFFIC MONITOR 9

2.1 Перехват объектов 11
2.2 Анализ объекта и вынесение решения по объекту 12
2.3 Ретроспективный анализ данных, решение пользователя по объекту 16
2.4 Транспортные режимы InfoWatch Traffic Monitor 17
2.5 Загрузка объекта в базу данных 18
2.6 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов 18

3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ С КОНСОЛЬЮ УПРАВЛЕНИЯ 20

3.1 Работа Системы до конфигурирования 21
3.2 Работа с конфигурацией Системы 22
3.3 Отображение актуальных данных в Консоли управления 23

4 ИНТЕРФЕЙС КОНСОЛИ УПРАВЛЕНИЯ 25

4.1 Раздел "Сводка" 28
4.1.1 Панели 29
4.1.2 Виджеты сводки 30
4.1.2.1 Динамика нарушений за период 30
4.1.2.2 Топ нарушителей 31
4.1.2.3 Количество нарушений за период 33
4.1.2.4 Подборка 34
4.1.2.5 Динамика статусов за период 35
4.1.2.6 Статистика по политикам 36
4.1.2.7 Статистика по объектам защиты 36
4.1.2.8 Статистика по каталогам объектов защиты 38
4.1.3 Выгрузка сводки 39
4.2 Раздел "События" 40
4.2.1 Запросы 42
4.2.1.1 Условие 43
4.2.1.2 Поля просмотра 47
4.2.1.3 Параметры доступа 48
4.2.1.4 Расширенный режим редактирования запроса 48
4.2.1.5 Поиск по тексту события 49
4.2.2 Объекты перехвата 52
4.2.2.1 Плитка события 54
4.2.2.2 Краткая форма просмотра событий 55
4.2.2.3 Детальная форма просмотра событий 57
4.2.3 Идентификация контактов в событии 58
4.3 Раздел "Отчеты" 59
4.3.1 Виджеты отчетов 60
4.3.2 Запросы 63
4.3.3 История выполнения отчета 64
4.3.4 Форма создания отчета 65
4.3.5 Форма создания папки с отчетами 65
4.4 Раздел "Технологии" 66
4.4.1 Категории и термины 67
4.4.1.1 Категории 68
4.4.1.2 Термины 70

4.4.2 Текстовые объекты ... 71
4.4.2.1 Шаблоны текстовых объектов ... 72
4.4.3 Эталонные документы ... 74
4.4.4 Бланки ... 76
4.4.5 Печати ... 79
4.4.6 Выгрузки из БД ... 80
4.4.6.1 Автоматически обновляемые выгрузки из БД ... 83
4.4.7 Графические объекты ... 84
4.5 Раздел "Объекты защиты" ... 85
4.5.1 Элементы анализа ... 87
4.5.2 Условия обнаружения ... 87
4.6 Раздел "Персоны" ... 89
4.6.1 Группы персон и рабочих станций ... 91
4.6.2 Персоны ... 92
4.6.3 Рабочие станции ... 94
4.7 Раздел "Политики" ... 95
4.7.1 Политики и форма их просмотра ... 97
4.7.2 Правила и форма их просмотра ... 98
4.7.2.1 Правило передачи ... 99
4.7.2.2 Правило копирования ... 102
4.7.2.3 Правило хранения ... 103
4.7.2.4 Правило контроля персон ... 104
4.7.3 Область "Настройка фильтра" ... 105
4.7.4 Окно добавления политики ... 105
4.8 Раздел "Списки" ... 106
4.8.1 Теги ... 107
4.8.2 Список ресурсов ... 108
4.8.3 Статусы ... 109
4.8.4 Периметры ... 110
4.8.5 Список файлов ... 111
4.9 Раздел "Краулер" ... 112
4.9.1 Сканер ... 115
4.9.2 Задание на сканирование ... 116
4.9.3 История запусков ... 120

5 РЕШЕНИЕ ЗАДАЧ ... 122

5.1 Типовые действия ... 122
5.1.1 Вход в Консоль управления и выход из нее ... 123
5.1.2 Применение конфигурации Системы ... 124
5.1.3 Редактирование элемента ... 125
5.1.4 Удаление элемента ... 125
5.1.5 Навигация по страницам ... 125
5.1.6 Изменение пароля пользователя ... 126
5.1.7 Выбор языка интерфейса ... 127
5.1.8 Вызов справки ... 127
5.1.9 Просмотр сведений о Системе ... 127
5.2 Работа с персонами и рабочими станциями ... 128
5.2.1 Создание группы персон и рабочих станций ... 128
5.2.2 Создание персон и рабочих станций ... 129
5.2.3 Просмотр событий по персоне ... 130
5.2.4 Просмотр сводки по персоне ... 131
5.2.5 Добавление статуса персонам ... 131
5.2.6 Добавление персоны в периметр ... 132
5.2.7 Настройка карточки персоны ... 132
5.2.7.1 Добавление персоне контакта ... 133
5.2.7.2 Добавление персоне рабочей станции ... 134

5.2.7.3 Добавление персоны в группу ... 134
5.2.8 Настройка карточки компьютера ... 135
5.2.8.1 Добавление компьютеру контакта ... 136
5.2.8.2 Добавление компьютеру персоны ... 136
5.2.8.3 Добавление компьютера в группу ... 137
5.3 РАБОТА СО СПРАВОЧНИКАМИ ... 138
5.3.1 Работа с тегами ... 138
5.3.2 Работа со веб-ресурсами ... 139
5.3.3 Работа со статусами ... 140
5.3.4 Работа с периметрами ... 141
5.4 РАБОТА С БАЗОЙ ТЕХНОЛОГИЙ ... 144
5.4.1 Определение конфиденциальной информации ... 144
5.4.1.1 Работа с категориями и терминами ... 146
5.4.1.1.1 1. Создание категории. ... 146
5.4.1.1.2 2. Создание термина. ... 147
5.4.1.2 Работа с текстовыми объектами ... 149
5.4.1.2.1 1. Создать каталог текстовых объектов. ... 149
5.4.1.2.2 2. Создание текстового объекта и указание его значения. ... 149
5.4.1.3 Работа с эталонными документами ... 151
5.4.1.4 Работа с бланками ... 154
5.4.1.5 Работа с печатями ... 155
5.4.1.6 Работа с выгрузками ... 156
5.4.1.6.1 Условия детектирования выгрузки ... 158
5.4.2 Экспорт и импорт базы технологий ... 161
5.5 РАБОТА С ОБЪЕКТАМИ ЗАЩИТЫ ... 162
5.5.1 Создание каталога объектов защиты ... 163
5.5.2 Создание объекта защиты ... 164
5.5.3 Добавление элементов анализа ... 166
5.5.4 Добавление условий обнаружения ... 167
5.5.5 Создание политики для объектов защиты и их каталогов ... 168
5.5.6 Импорт и экспорт объектов защиты ... 169
5.5.7 Активация и деактивация объектов защиты ... 170
5.6 РАБОТА С ПОДСИСТЕМОЙ КРАУЛЕР ... 171
5.6.1 Настройка сканера ... 172
5.6.2 Создание задачи ... 173
5.6.3 Запуск и остановка задачи ... 174
5.6.4 Редактирование задачи ... 174
5.6.5 Очистка хеша ... 174
5.6.6 Просмотр истории запусков ... 175
5.6.7 Сохранение отчета ... 176
5.7 РАБОТА С ОБЪЕКТАМИ ПЕРЕХВАТА ... 176
5.7.1 Просмотр сводки по нарушениям/нарушителям ... 177
5.7.1.1 Создание панели ... 177
5.7.1.2 Создание виджета ... 177
5.7.1.3 Настройка виджета ... 179
5.7.2 Просмотр событий ... 179
5.7.2.1 Создание запросов ... 180
5.7.2.1.1 Создание запроса в стандартном режиме ... 180
5.7.2.1.2 Создание запроса в расширенном режиме ... 181
5.7.2.1.3 Использование расширенного синтаксиса ... 185
5.7.2.2 Выбор полей просмотра событий ... 186
5.7.2.3 Просмотр краткой формы события ... 187
5.7.2.4 Просмотр детальной формы события ... 187
5.7.3 Работа с выгрузками сводки ... 188
5.7.3.1 Создание выгрузки сводки ... 188
5.7.3.2 Просмотр выгрузки сводки ... 190
5.7.4 Вынесение решения по объекту ... 191
5.7.5 Добавление и удаление тега ... 191

5.7.6 Сохранение события (для SMTP-писем) ... 192
5.7.7 Выгрузка события ... 192
5.7.8 Досылка события, находящегося в карантине ... 193
5.8 Настройка реакций Системы ... 194
5.8.1 Общие сведения о политиках ... 195
5.8.1.1 Разбиение события на суб-события ... 196
5.8.1.2 Разбиение правил на суб-правила ... 196
5.8.1.3 Определение приоритетного суб-правила ... 197
5.8.1.4 Порядок применения действий согласно отобранным приоритетным правилам ... 198
5.8.1.5 Пример: ... 199
5.8.2 Предустановленные политики ... 200
5.8.2.1 Политики защиты конфиденциальных данных ... 201
5.8.2.2 Политика контроля персон ... 202
5.8.2.2.1 Правила политики ... 202
5.8.2.3 Политика, регулирующая передачу данных, защищенных паролем ... 202
5.8.2.3.1 Правила политики ... 203
5.8.2.4 Политики, контроллирующие посещение веб-ресурсов ... 203
5.8.2.4.1 Нецелевое использование ресурсов ... 203
5.8.2.4.1.1 Правила политики ... 203
5.8.2.4.2 Нелояльные сотрудники ... 204
5.8.2.4.2.1 Правила политики ... 204
5.8.2.4.3 Скрытие действий сотрудников ... 204
5.8.2.4.3.1 Правила политики ... 205
5.8.2.4.4 Подозрительная активность ... 205
5.8.2.4.4.1 Правила политики ... 205
5.8.3 Создание политики защиты данных ... 205
5.8.4 Создание политики контроля персон ... 206
5.8.5 Редактирование политики ... 208
5.8.6 Создание правил ... 208
5.8.7 Редактирование правил ... 210
5.8.8 Определение действий Системы в случае нарушения правил ... 210
5.8.9 Определение действий Системы по умолчанию ... 212
5.8.10 Фильтрация списка политик ... 213
5.8.11 Отправка уведомлений о сработавшем правиле ... 213
5.9 Работа с отчетами ... 215
5.9.1 Создание папки с отчетами ... 215
5.9.2 Создание отчета ... 216
5.9.3 Работа с виджетами отчетов ... 217
5.9.3.1 Создание и настройка виджета ... 217
5.9.4 Работа с готовыми отчетами ... 218

6 ЛИЦЕНЗИОННАЯ ИНФОРМАЦИЯ ... 220

6.1 Пользовательское лицензионное соглашение ... 220
6.1.1 Лицензионное соглашение ... 220
6.1.1.1 1. Определения ... 220
6.1.1.2 2. Предоставление лицензии ... 221
6.1.1.3 3. Ограничения ... 221
6.1.1.4 4. Ограниченная гарантия и отказ от предоставления гарантий ... 222
6.1.1.5 5. Ограничение ответственности ... 222
6.1.1.6 6. Программные продукты ... 223
6.1.1.7 7. Открытое (свободное) программное обеспечение ... 223
6.1.1.8 8. Права на интеллектуальную собственность ... 223
6.1.1.9 9. Контактная информация Правообладателя ... 223
6.2 Лицензии третьих сторон ... 224

7 ГЛОССАРИЙ ... 225

1 ВВЕДЕНИЕ

InfoWatch Traffic Monitor (далее Traffic Monitor или Система) – это распределенная многокомпонентная система, предназначенная для контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, ICQ, NRPC). Кроме того, InfoWatch Traffic Monitor выполняет анализ данных, полученных от системы InfoWatch Device Monitor.

Веб-консоль управления (далее Консоль управления) является частью системы InfoWatch Traffic Monitor, позволяет управлять настройками и осуществлять мониторинг работы Системы.

Веб-консоль управления имеет интуитивно понятный интерфейс, поэтому настоящее руководство содержит только общую информацию и ряд наглядных примеров, которые дают возможность представить весь функционал Системы.

1.1 Аудитория

Информация, содержащаяся в руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

1.2 Комплект документов

В комплект документации по InfoWatch Traffic Monitor входят:

- «*InfoWatch Traffic Monitor. Руководство пользователя*».

Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).

- «*InfoWatch Traffic Monitor. Руководство администратора*».

Содержит информацию по администрированию Системы (база данных, серверная часть).

- *«InfoWatch Traffic Monitor. Руководство по установке»*

Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.

1.3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы Службы технической поддержки – с 7-00 до 21-00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ.
Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/support.html.
Перед обращением в службу технической поддержки мы рекомендуем вам посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

2 ОБЗОР INFOWATCH TRAFFIC MONITOR

InfoWatch Traffic Monitor позволяет контролировать информационные потоки в корпоративной среде для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

Основные функции InfoWatch Traffic Monitor:

- Перехват SMTP, IMAP и POP3-трафика. Возможен перехват трафика (или копии трафика), передаваемого через почтовый relay-сервер; перехват копии трафика, проходящего через управляемый коммутатор.
- Перехват HTTP- и HTTPS-трафика. Возможен перехват трафика, передаваемого через прокси-сервер, поддерживающий ICAP-протокол; перехват копии трафика, проходящего через управляемый коммутатор.

> **Примечание:**
>
> Перехват HTTPS-трафика возможен при интеграции с прокси-сервером Blue Coat, если прокси-сервер обрабатывает HTTPS-трафик как HTTP-трафик.

- Перехват копии ICQ-трафика (протокол OSCAR), проходящего через управляемый коммутатор. При подключении ICQ через HTTP Система перехватывает ICQ-трафик аналогично HTTP-трафику.

> **Важно!**
>
> Система не поддерживает перехват и анализ зашифрованного ICQ-трафика, в том числе трафика, передаваемого по зашифрованному протоколу SSL.

- Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint 2007/2010/2013), с помощью подсистемы Crawler.
- Анализ Skype-, Yahoo- трафика, теневых копий файлов и заданий на печать, фотографий, передачи трафика по протоколам HTTP, HTTPS и FTP, приема и передачи электронных писем по протоколам SMTP, POP3, IMAP и с помощью интерфейса MAPI, контроль обмена данными через Jabber (протокол XMPP), Mail.Ru Агент (протокол MMP), WhatsApp (протокол WhatsApp) и с помощью SMS. Перехват перечисленных данных осуществляется системой InfoWatch Device Monitor.
- Анализ теневых копий файлов, перехваченных системой DeviceLock ЗАО «Смарт Лайн Инк» (версии 6.3 и выше).
- Перехват и анализ объектов MS Lync при помощи IW Lync Adapter, который устанавливается на MS Lync сервер.

- Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности.
- Фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

> **Важно!**
>
> Функция недоступна при работе с копией трафика.

Состав InfoWatch Traffic Monitor:

Компонент InfoWatch Traffic Monitor	Назначение компонента
Сервер Traffic Monitor	**IW_SNIFFER**, **IW_ICAP** и **IW_SMTPD** - перехватчики. **Подсистема анализа**: получение контекста события и проверка на содержание элементов технологий и на соответствие объектам защиты. **Подсистема применения политик**: выполнение действий, заданных пользователем согласно корпоративной политике безопасности.
База данных	Хранение информации, связанной с работой Системы (перехваченные данные и результаты их анализа).
Device Monitor	Контроль доступа пользователей к периферийным устройствам, мониторинг операций (копирование данных на съемные носители и FTP, отправка данных на печать, использование мессенджеров) и перехват трафика систем мгновенного обмена сообщениями.
Crawler	Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint).
Коннекторы	Интеграция со сторонними системами, формирование событий.
Консоль управления	Настройка правил анализа и фильтрации трафика, анализ полученных данных.

Описание основ работы Системы содержится в следующих вводных разделах:

- Перехват объектов
- Транспортные режимы InfoWatch Traffic Monitor
- Анализ объекта и вынесение вердикта
- Загрузка объекта в базу данных
- Ретроспективный анализ данных, решение пользователя по объекту

- Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов

2.1 Перехват объектов

Под *объектами* в Системе понимаются:

- объекты трафика (SMTP-, IMAP4- и POP3-письма, HTTP- и HTTPS-запросы, файлы фотографий, ICQ-сообщения, сообщения Skype, Yahoo, XMPP, MS Lync, WhatsApp, Mail.Ru Агент и SMS-сообщения);
- теневые копии файлов;
- задания на печать.

Возможно несколько вариантов перехвата в зависимости от типа объектов:

Тип объекта	**Варианты перехвата объектов**
SMTP, IMAP и POP3	• Система выполняет перехват и доставку SMTP-, IMAP- и POP3-трафика. Возможна фильтрация перехваченных объектов (разрешение/запрещение доставки). • Система получает копию SMTP-, IMAP- и POP3-трафика от корпоративного почтового relay-сервера. Система не участвует в доставке трафика. • Система получает копию SMTP-, IMAP- и POP3-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика.
HTTP	• Система перехватывает HTTP-трафик путем интеграции с ICAP-сервером. Возможна фильтрация перехваченных объектов (разрешение/запрещение) доставки. • Система получает копию HTTP-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика.
HTTPS	Система получает копию трафика от InfoWatch Device Monitor.
MAPI	Система получает копию трафика от InfoWatch Device Monitor.
FTP	Система получает копию трафика от InfoWatch Device Monitor.

Тип объекта	Варианты перехвата объектов
ICQ	• Система получает копию ICQ-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика. • При подключении ICQ через HTTP Система перехватывает ICQ-трафик аналогично трафику HTTP.
Сообщения Skype, Yahoo, Mail.Ru Агент, WhatsApp	Система получает копию трафика Skype, Yahoo, Mail.Ru Агент, WhatsApp от InfoWatch Device Monitor.
SMS-сообщения	Система получает копию SMS-сообщений от InfoWatch Device Monitor.
Фотографии	Система получает копию файла мультимедиа от InfoWatch Device Monitor.
MS Lync	Система получает копию объектов от IW Lync Adapter, установленного на сервере MS Lync.
Файлы, расположенные в корпоративной сети	Система получает копии файлов от подсистемы Crawler.
Теневые копии файлов и задания на печать, полученные от InfoWatch Device Monitor	Система получает копию трафика. Блокирование действий пользователя (печать, доступ к устройствам) доступно только через InfoWatch Device Monitor.
Теневые копии файлов, полученные от DeviceLock	Система получает копию трафика. Блокирование действий пользователя (доступ к устройствам) доступно только через DeviceLock

Варианты перехвата и последующая доставка объектов определяются транспортными режимами InfoWatch Traffic Monitor.

2.2 Анализ объекта и вынесение решения по объекту

Обработка и анализ перехваченных объектов, а также применение к ним политик безопасности, осуществляется следующими подсистемами InfoWatch Traffic Monitor:

Подсистема IW TM	Модули подсистемы	Функции подсистемы/модуля

Подсистема IW TM	Модули подсистемы	Функции подсистемы/модуля
Подсистема Обработки	Модуль Обработки SMTP- и POP3-трафика (режим копии), Модуль Обработки HTTP-трафика (режим копии), Модуль Обработки ICQ-трафика (режим копии), Модуль Обработки Теневых Копий, Модуль Обработки SMTP-трафика (блокирующий режим), Модуль Обработки HTTP-трафика (блокирующий режим)	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в Подсистему Анализа.
Подсистема Анализа	Модуль Лингвистического Анализа	Проверка текста на соответствие каким-либо категориям.
	Модуль Детектирования Текстовых Объектов	Поиск текстовых объектов (например, номеров кредитных карт) в тексте объектов.
	Модуль Детектирования Цифровых Отпечатков	Поиск цитат из эталонных документов в тексте объектов.
	Модуль Детектирования Бланков	Поиск бланков в тексте объектов.
	Модуль Детектирования Печатей	Поиск изображений печатей в тексте объектов.
	Модуль Детектирования Выгрузок из БД	Поиск цитат из базы данных в тексте событий.
	Модуль Детектирования Графических Объектов	Поиск изображений, принадлежащих определенным классам, в тексте и вложениях объектов.
Подсистема Применения Политик	Модуль Интеграции с Active Directory и Domino Directory	Обеспечение первоначального импорта и периодической синхронизации структуры каталога Active Directory и Domino Directory со справочником персон и рабочих станций для выполнения дальнейшей привязки этой информации к данным из перехваченных объектов.
	Модуль Принятия Решений	Обеспечение корпоративной политики безопасности путем выполнения для объектов правил из набора политик.

Анализ объекта выполняется в следующем порядке:

1. **Выделение атрибутов объекта** – Подсистема Обработки выделяет у объектов имеющиеся атрибуты. Например, у SMTP-писем – адреса отправителя и получателей, тема письма и т.п. Перечень возможных атрибутов объекта приведен в статье "Плитка события".

2. **Извлечение вложенных файлов** – Модуль Принятия Решений анализирует вложенные файлы на основании таких атрибутов, как название и формат файла.
3. **Анализ текста и графических объектов** – Подсистема Анализа обрабатывает текстовые и графические данные: тексты писем, сообщений, запросов; тексты, извлеченные из вложений поддерживаемых форматов, а также файлы изображений.

Примечание.

Для документов MS Office 2007 и 2010 анализируются также метаданные, указанные в свойствах документа (вкладка **Подробно**, блок **Описание**).

В Системе предусмотрены несколько видов анализа, доступность которых зависит от приобретённой лицензии на продукт:

Технология контентного анализа	**Описание технологии**
Лингвистический анализ	Определение тематики и содержания текста по терминам (словам и словосочетаниям), найденным в тексте. Поиск терминов выполняется на основе базы категорий и терминов, отражающих специфику организации. Все термины распределены по категориям (каждый термин можно соотнести с одной или несколькими категориями). Таким образом, наличие термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией. Например, термин *Заработная плата* может принадлежать сразу нескольким категориям (*Внутренние выплаты*, *Условия труда*). Присутствие в тексте этого термина означает, что текст может принадлежать к указанным категориям.
Детектирование текстовых объектов	Поиск текстовых объектов, соответствующих заданным шаблонам (например, поиск номеров кредитных карт в текстах перехваченных объектов)
Детектирование цифровых отпечатков	Поиск фрагментов текста, принадлежащих к заранее заданным эталонным документам (например, тексты приказов, финансовых отчетов, договоров и пр.)
Детектирование бланков	Поиск бланков установленного шаблона. Бланками могут быть различные анкеты, квитанции и проч.
Детектирование паспортов граждан РФ	Поиск изображений паспортов граждан РФ. Технология работает при включенном текстовом объекте *Паспорт гражданина РФ*
Детектирование печатей	Поиск изображения печати установленного вида. Эталонными печатями могут быть изображения круглых оттисков, которые используются в организациях
Детектирование выгрузок из БД	Поиск цитат из заданной базы данных. Эталонными выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и проч.
Детектирование графических объектов	Поиск изображений, соответствующих какой-либо из предустановленных категорий. К графическим объектам относятся изображения паспортов, кредитных карт и проч.

- На основании результатов анализа Модуль Принятия Решений выносит заключение о возможном нарушении политики информационной безопасности и определяет, какие действия должны быть выполнены в случае нарушения. Правила, определяющие действия Системы в случае нарушения, задаются в политике. Предусмотрены следующие действия (набор возможных действий определяется типом правила):
    - **Назначить событию уровень нарушения**. Возможные значения: **Высокий**, **Средний**, **Низкий**, **Отсутствует**.
    - **Назначить персонам статус**. Статус, который будет присвоен нарушителям (подробнее см. "Статусы").
    - **Назначить событию теги**. Теги, которые будут назначены событию в случае нарушения политики (подробнее см. "Теги").
    - **Назначить событию вердикт**. Решение Системы, является ли событие потенциальным нарушением. Возможные значения: **Разрешить**, **Заблокировать**, **Поместить на карантин**.
    - **Удалить событие**. Событие не будет сохранено в базу данных.

2.3 Ретроспективный анализ данных, решение пользователя по объекту

Объекты, хранящиеся в базе данных, доступны для анализа в Консоли управления. При этом пользователь может просматривать результаты анализа, проведенного Системой, и выносить собственное решение по объекту (атрибут *Решение*).
Первоначально атрибут *Решение* у каждого объекта имеет значение *Решение не принято*. Затем пользователь может вынести по объекту одно из следующих решений:

- *Нарушение*. По результатам анализа пользователь пришел к выводу, что объект нарушает корпоративную политику безопасности.
- *Нет нарушения*. Пользователь проанализировал объект и пришел к выводу, что объект не нарушает корпоративную политику безопасности.
- *Решение не принято*. Пользователь проанализировал объект и не пришел к выводу, нарушает ли объект корпоративную политику безопасности.
- *Требуется дополнительный анализ*. Пользователь проанализировал объект и решил, что для принятия решения требуются дополнительные действия.

В результате решения пользователя также может измениться вердикт, вынесенный событию Системой (см. "Вынесение решения по объекту"), и статус отправки SMTP-письма (см. "Досылка события, находящегося в карантине").

Примечание:

При работе системы "*В разрыв"* при назначении вердикта *Разрешено*, письмо покидает периметр компании вне зависимости от дальнейшего редактирования решения.

2.4 Транспортные режимы InfoWatch Traffic Monitor

Система InfoWatch Traffic Monitor имеет два транспортных режима: *Копия* и *Блокировка*. Условия, в соответствии с которыми определяется транспортный режим, задаются при настройке перехватчиков (подробнее см. документ *"Infowatch Traffic Monitor. Руководство администратора".* Действия, связанные с транспортировкой объекта, выполняются с учетом выбранного транспортного режима.

В таблице 1 приведены допустимые транспортные режимы для объектов разного типа. Различие между режимами работы заключается в особенностях транспортировки объектов (см. таблицу 2).

Табл. 1

Транспортный режим	**Описание**
Блокировка	Перехват, анализ и дальнейшая транспортировка объектов выполняются посредством Системы InfoWatch Traffic Monitor. В этом режиме возможность доставки объекта получателям определяется вердиктом, вынесенным объекту. Кроме того, в некоторых случаях состояние доставки SMTP-писем может изменяться после смены решения пользователя (см. "Досылка события, находящегося в карантине").
Копия	В данном режиме Система получает копии объектов. Отличие режима *Копия* от режима *Блокировка* заключается в том, что транспортировка объектов выполняется без участия Системы. Таким образом, задачей Системы является только анализ объектов. Поскольку анализ выполняется для копии объекта, то вердикт и решение пользователя, вынесенные по результатам анализа, не оказывают влияния на доставку этого объекта получателям.

Табл. 2

Тип объекта	**Транспортный режим "Блокировка"**	**Транспортный режим "Копия"**
SMTP	Да	Да (для копии трафика, полученной от почтового relay-сервера или от Sniffer)
HTTP-запрос	Да (только при перехвате трафика по протоколу ICAP)	Да
ICQ-сообщение	Нет	Да (только для копии трафика, полученной от Sniffer)
Сообщение Skype, Yahoo, Jabber, Mail.Ru Агент или WhatsApp	Нет	Да
SMS-сообщение	Нет	Да
MS Lync	Нет	Да
Теневая копия файла	Нет	Да
Фотосъемка	Нет	Да

2.5 Загрузка объекта в базу данных

После того как объект проанализирован и по нему принято решение Системы (подробнее см. "Анализ объекта и вынесение решения по объекту"), в базу данных загружается объект и XML-контекст объекта. XML-контекст включает в себя:

- данные (атрибуты, текст), извлеченные из объекта, в том числе из вложений объекта;
- результаты анализа объекта;
- информацию о решении по объекту.

2.6 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов

Если в нормальном транспортном режиме (см. "Транспортные режимы InfoWatch Traffic Monitor") Система принимает решение о блокировке HTTP-запроса или письма, отправляемого с помощью веб-сервиса (например, *mail.ru*), то в браузере пользователя, отправившего запрос или письмо, отобразится сообщение о блокировке.
Если отправка почты выполняется через почтовые сервисы, построенные по технологии AJAX (такие как Gmail, Windows Live Hotmail и др.), то пользователю может не выдаваться сообщение о том, что доставка письма заблокирована. Как правило, в таких случаях выдается сообщение, определенное самим почтовым сервисом.
POST-запросы на ряд веб-ресурсов (см. таблицу ниже) Система обрабатывает в соответствии со специальными правилами:

- на панели информации об объекте (см. "Объекты перехвата") отображаются атрибуты *От*, *Кому*, *Копия*, *Тема* и *Отправлено*, а также вложения (в случае их наличия);
- запросы, для которых нельзя определить эти атрибуты и выделить в их заголовках какой-либо текст, можно удалять как "мусорный" трафик. Таким мусорным трафиком являются, например, фоновые запросы для обновления статуса в социальных сетях.

Перехват HTTP/HTTPS-запросов поддерживает форумы на базе IP Board, phpbb и vBulletin.

Поддерживаемые веб-ресурсы:

Тип веб-ресурса	**Ресурсы**	
Без ограничений	**С ограничениями**	
Веб-почта	mail.ru, mail.yandex.ru, rambler.ru, pochta.ru, km.ru, newmail.ru, gmail.com, inbox.com, hotmail.com, hotmail.ru, mail.com, live.com	yahoo.com, mail.com, aol.com, gmx.com
Интернет-дневники и социальные сети	facebook.com, blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, perfspot.com	myspace.com, blogger.com, vkontakte.ru (vk.com), odnoklassniki.ru, twitter.com, livejournal.com (.ru), wordpress.com, linkedin.com

Тип веб-ресурса	Ресурсы	
Сайты поиска работы и размещения резюме		moikrug.ru, hh.ru, job.ru, rabota.ru, jobs.com, eurojobs.com
Форумы	forum.ru-board.com, sysadmins.ru, talk.mail.ru, dom.bankir.ru, biznet.ru	forum.ixbt.com, groups.google.ru (.com)

Также поддерживаются следующие файловые хранилища и хостинги**:** blogspot, google drive, cloud.mail.ru, disk.yandex.ru, mail.qip.ru, file.qip.ru, onedrive.live.com, google plus, talk.mail.ru.

3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ С КОНСОЛЬЮ УПРАВЛЕНИЯ

Для работы в Консоли управления требуется наличие постоянного соединения с сервером базы данных. Чтобы подключиться к серверу базы данных, пользователю необходимо выполнить процедуру авторизации.

При авторизации проверяется выполнение следующих условий:

- в базе данных существует учетная запись с указанными параметрами;
- учетная запись не заблокирована.

Если хотя бы одно из условий не соблюдается, пользователь не сможет авторизоваться в Системе.

Если авторизация прошла успешно, пользователь получит доступ к главному окну Консоли управления. В противном случае на экран будет выведено сообщение об ошибке.

В зависимости от того, какая роль назначена учетной записи, от имени которой производится вход в Систему, пользователь может иметь разные права:

- Администратор - роль, имеющая все необходимые права для первичной настройки Консоли управления.
- Офицер безопасности (ОБ) - роль, обладающая всеми привилегиями, кроме первичной настройки Консоли управления.

Примечание:

В настоящем руководстве не описываются алгоритмы действий Администратора. Вся необходимая информация по этому вопросу содержится в документе «*Infowatch Traffic Monitor. Руководство администратора*».

После того, как вход выполнен, пользователь может сконфигурировать Систему (о работе Системы сразу после установки см. "Работа Системы до конфигурирования"). Конфигурация Системы состоит из следующих действий:

- настройка базы технологий;
- составление справочников;
- создание объектов защиты;
- настройка реакций Системы на действия персон, нарушающие корпоративную политику безопасности.

Настройка конфигурирования Системы завершается применением обновленной конфигурации (см. "Работа с конфигурацией Системы").

Примечание:

Если Система уже сконфигурирована ранее, и задачи пользователя обеспечиваются примененной конфигурацией, дополнительного конфигурирования Системы не требуется.

Список типовых действий пользователя приведен в разделе "Решение задач". После завершения конфигурирования Системы офицер безопасности может просмотреть сводку о нарушениях правил корпоративной безопасности (см. "Работа с объектами перехвата").

Также пользователь имеет возможность настраивать внешний вид Консоли управления и выполнять другие задачи.

Если с Консолью управления одновременно работает несколько пользователей, то для получения актуальных данных следует применять обновление данных (см. "Отображение актуальных данных в Консоли управления").

Важно!

Для корректной работы Системы требуется, чтобы в антивирусных программах и другом блокирующем ПО не блокировался интернет-контент.
Например, в антивирусе G DATA Security требуется снять флажок в поле **Process Internet content (HTTP)**.

3.1 Работа Системы до конфигурирования

Установленная Система, для которой еще не выполнялось конфигурирование (о конфигурировании Системы см. "Решение задач"), функционирует следующим образом:

- Осуществляет перехват трафика и проверку объектов перехвата на соответствие установленным категориям. В случае соответствия объекта перехвата какой-либо категории, Система присваивает объекту соответствующий атрибут.
- Позволяет пользователю войти в Систему, используя одну из предустановленных учетных записей:
  - **Administrator** (роль Администратор);
  - **Officer** (роль Офицер безопасности).
- Отображает в Консоли управления информацию об объектах перехвата. Чтобы отображать информацию об отправителях и получателях трафика, необходимо выполнить настройку списков персон и рабочих станций (см. "Работа с персонами и рабочими станциями").
- Сохраняет в базу данных объекты перехвата. При этом никаких действий по отношению к объектам в процессе анализа не предпринимается. Чтобы указать, какие действия требуется выполнять с объектами перехвата, необходимо настроить периметр компании (см. "Работа с периметрами"). После этого при анализе объектов перехвата Система будет применять действия, заданные в политиках по умолчанию.

3.2 Работа с конфигурацией Системы

Конфигурация представляет собой набор различных настроек, необходимых для проверки объектов на сервере Traffic Monitor, а также для мониторинга и анализа данных.

Каждый объект, передаваемый в Traffic Monitor, обрабатывается в соответствии с той версией конфигурации, которая в данный момент действует на сервере, а затем сохраняется в базу данных вместе со всеми атрибутами, присвоенными данному объекту по результатам обработки.

Важно!

Система не выполняет повторную обработку объекта по новой, измененной конфигурации.

Настройка конфигурации включает в себя:

- Составление базы элементов технологий (см. "Настройка базы технологий"):
  - выбор терминов, подлежащих детектированию - *только при использовании технологии Лингвистический анализ (см. "Термины")*;
  - выбор типов текстовых объектов, подлежащих детектированию - *только при использовании технологии Детектирование текстовых объектов (см. "Текстовые объекты")*;
  - выбор эталонных документов, подлежащих детектированию - *только при использовании технологии Детектирование эталонных документов (см. "Эталонные документы")*;
  - выбор эталонных бланков, подлежащих детектированию - *только при использовании технологии Детектирование эталонных бланков (см. "Бланки")*;
  - выбор эталонных печатей, подлежащих детектированию - *только при использовании технологии Детектирование эталонных печатей (см. "Печати")*;
  - выбор выгрузок из БД, подлежащих детектированию - *только при использовании технологии Детектирование выгрузок из БД (см. "Выгрузки из БД")*;
  - выбор типов графических объектов, подлежащих детектированию - *только при использовании технологии Детектирование графических объектов (см. "Графические объекты").*
- Создание объектов защиты на основе элементов базы технологий *(см. "Объекты защиты")*.
- Составление справочников:
  - персон и рабочих станций *(см. "Работа с персонами и рабочими станциями")*;
  - тегов *(см. "Работа с тегами")*;
  - списков ресурсов *(см. "Работа со списками ресурсов")*;
  - статусов *(см. "Работа со статусами")*;
  - периметров *(см. "Работа с периметрами")*;
- Составление политик, в соответствии с которыми будет выполняться проверка объектов на сервере Traffic Monitor *(см. "Настройка реакций Системы")*

После того как хотя бы один из приведенных выше параметров был изменен в Консоли управления, редактируемая версия конфигурации сохраняется в Системе. При этом:

- в верхней части рабочей области браузера пользователя, изменяющего конфигурацию, отображается сообщение типа:



- в верхней части рабочей области браузера пользователей, которым недоступно изменение конфигурации, отображается сообщение типа:
Конфигурация редактируется пользователем <security_officer> начиная с 15.06.2015 15:54

Важно!

До применения или сохранения конфигурации измененная версия доступна только пользователю, который ее изменяет. Другие пользователи Консоли управления работают с последней примененной конфигурацией Системы без права на ее изменение.

После завершения редактирования вы можете выбрать одно из действий:

- **Применить конфигурацию** (см. "Применение конфигурации Системы") - измененная конфигурация начнет действовать на сервере.
- **Сохранить конфигурацию** - измененная конфигурация станет доступна другим пользователям Консоли управления, но не будет использоваться в Системе для контроля трафика и анализа данных.
- **Отменить изменения** - конфигурация в Консоли управления будет соответствовать последней примененной на сервере конфигурации, и все сделанные изменения конфигурации удалятся. Для отмены изменений нажмите **Отменить** в появившемся окне списка изменений. В поле **Описание** при необходимости укажите причину отмены конфигурации. Эта информация будет сохранена в базе данных.

При интеграции с LDAP-каталогами, а также при добавлении новых контактов персон с помощью механизма пост-идентификации происходит автоматическое редактирование конфигурации. Обновление конфигурации выполняется независимо от ее текущего статуса.

Примечание.

Информация о контактах, добавленных в результате пост-идентификации, обновляется в Системе раз в 15 минут.

3.3 Отображение актуальных данных в Консоли управления

В Системе могут одновременно работать несколько пользователей. При этом каждому пользователю, работающему в Консоли управления, доступны данные из последней примененной

конфигурации (см. "Применение конфигурации Системы"), а также изменения, сделанные данным пользователем за текущую сессию редактирования конфигурации.

Для того чтобы поддерживать в актуальном состоянии сведения о Системе, необходимо периодически выполнять обновление данных. Обновление данных осуществляется автоматически и вручную.

Автоматическое обновление данных, относящихся к определенному разделу Консоли управления, выполняется при переходе к этому разделу. Вы можете также настроить обновление статистических данных о нарушениях/нарушителях.

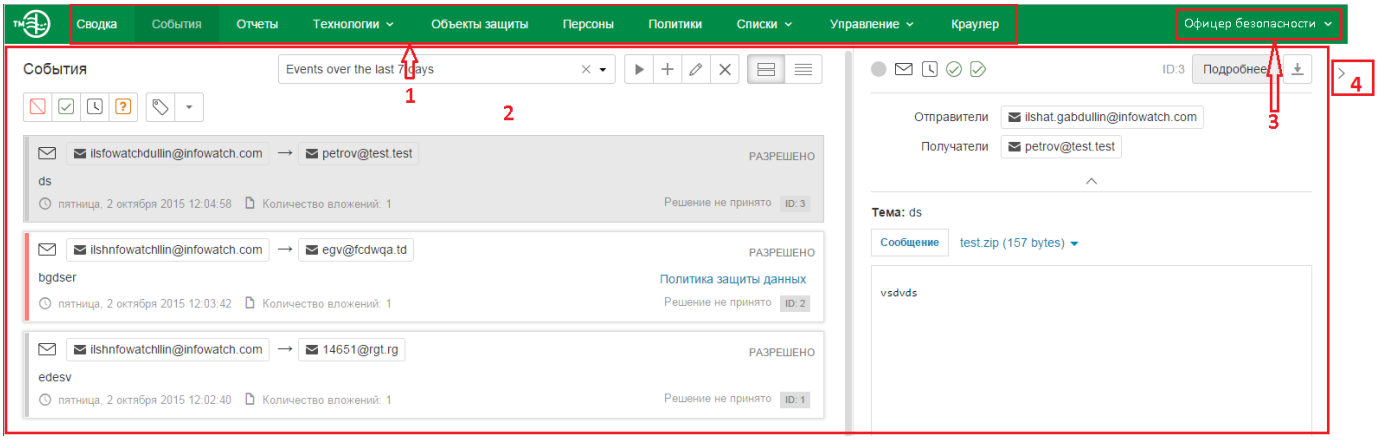
В любом из разделов Консоли управления вы также можете обновлять данные вручную. Для этого воспользуйтесь стандартным средством обновления страницы интернет-браузера (по умолчанию обновление выполняется при нажатии функциональной клавиши F5).

Примечание:

В тех случаях, когда запрашиваемые данные находятся в процессе загрузки, в Системе может отображаться символ вида  либо информационное сообщение.

4 ИНТЕРФЕЙС КОНСОЛИ УПРАВЛЕНИЯ

Все окна Консоли управления InfoWatch Traffic Monitor имеют ряд общих элементов.



Элементы окна Консоли управления:

Номер на схеме	Элемент окна консоли	Назначение элемента
1	Панель Навигации	Отображение кнопок разделов. При нажатии на кнопку раздела выполняется переход к выбранному разделу Консоли управления.
2	Рабочая область	Отображение элементов выбранного раздела Консоли управления, работа с элементами выбранного раздела.
3	Кнопка меню пользователя	Отображение имени пользователя. При нажатии раскрывается список, в котором пользователь может: • Сменить пароль своей учетной записи (см. "Изменение пароля пользователя") • Сменить язык интерфейса (см. "Выбор языка интерфейса ") • Вызвать справку по Системе (см. "Вызов справки") • Получить сведения о Системе (см. "Просмотр сведений о Системе") • Выполнить выход из Консоли управления (см. "Вход в Консоль управления и выход из нее")

4	Кнопка скрытия панели	Отображается в разделах, где рабочая область разделена на панели (например, список событий на панели в левой части рабочей области и информация о выбранном событии в правой). Позволяет скрыть панель для более удобного просмотра информации на других панелях. Повторное нажатие на кнопку (стрелочка при этом будет указывать в обратную сторону) восстанавливает скрытую панель.

Работа в Консоли управления ведется в тематических разделах:

Раздел	**Назначение**
Сводка	Раздел содержит статистическую информацию о нарушениях/нарушителях
События	Раздел содержит список объектов перехвата и средства для работы с ними
Отчеты	Раздел содержит выборку статистических данных о перехваченных объектах
Технологии	Раздел содержит описание используемых технологий анализа (категории и термины, текстовые объекты, эталонные документы и т.д.)
Объекты защиты	Раздел содержит список объектов защиты и средства для работы с ними
Персоны	Раздел содержит справочник персон и рабочих станций информационной системы организации, а также внешних контактов.
Политики	Раздел содержит список предполагаемых действий персон и алгоритм ответных действий Системы
Списки	Раздел содержит редактируемые справочники тегов, ресурсов, статусов и периметров
Управление	Работа в разделе описана в документе *«Infowatch Traffic Monitor. Руководство администратора»*
Краулер	Раздел содержит средства для создания, редактирования и запуска задач для подсистемы Краулер

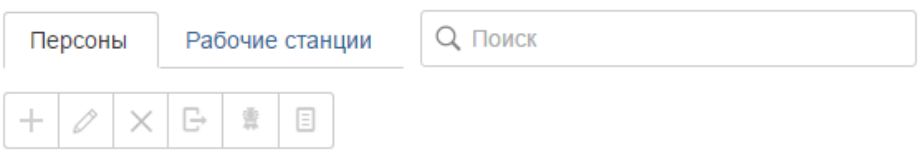
Переход к разделу происходит после нажатия на кнопку раздела.



Кнопка раздела **События**

В Консоли управления используются следующие элементы интерфейса:

- **Вкладка** - позволяет в одном окне переключение между несколькими определенными наборами элементов интерфейса.



Раздел **Персоны**, вкладки **Персоны** и **Рабочие станции**

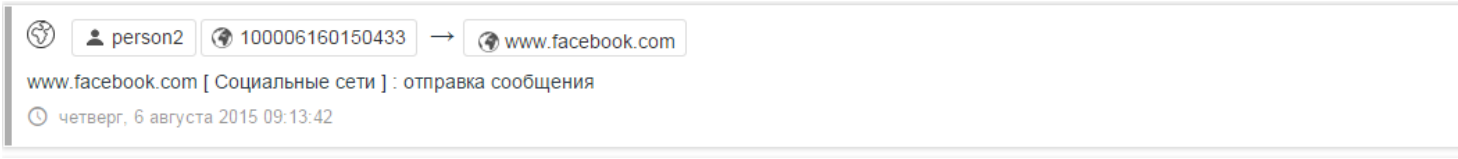
- **Панель** - область интерфейса, отображающая набор данных или содержащая набор элементов интерфейса, и отделенная от остальных областей.

> **Примечание:**
>
> Также *Панелью* в Системе называется сущность раздела **Сводка** (см. "Панели").



Панель инструментов

- **Часть рабочей области** - фрагмент рабочей области, обособленный от другого при помощи разделительной вертикальной линии.
- **Плитка** - весь набор данных для одной записи (все атрибуты объекта) в виде отдельного объекта.



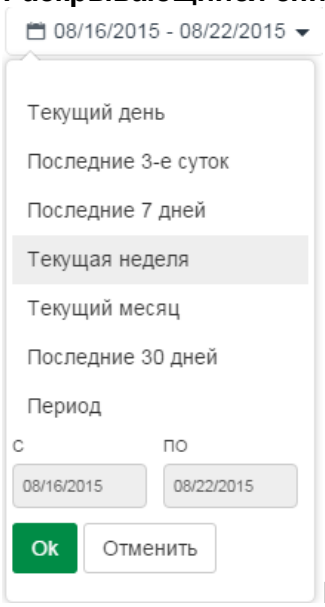
Раздел **События**, плитка события

- **Поле** - элемент для вывода строковых данных или для ввода данных с клавиатуры или из буфера обмена.



Поле **Поиск**

- **Раскрывающийся список** - отражает список элементов при нажатии.



Раздел **Сводка**, раскрывающийся список на виджете

Вы можете настраивать интерфейс Консоли управления (подробную информацию см. в тематических разделах).

Примечание:

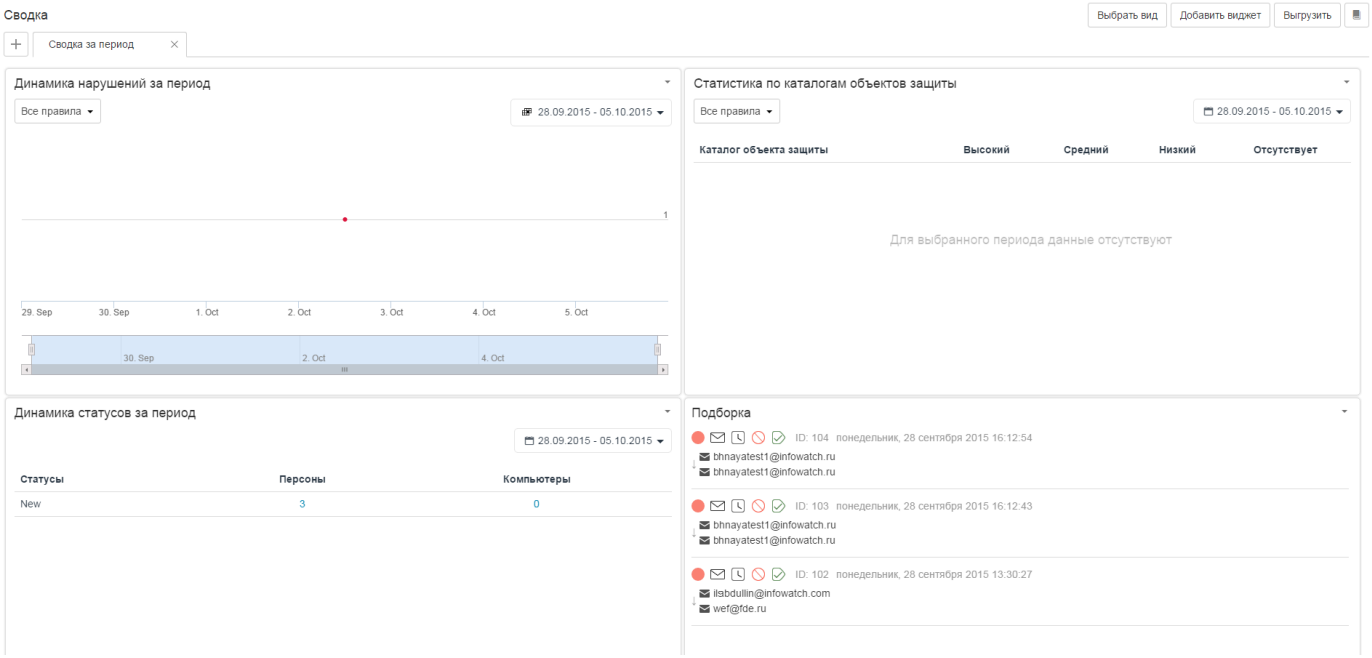
В тех случаях, когда запрашиваемые данные находятся в процессе загрузки, в Системе может отображаться символ вида  либо информационное сообщение.

4.1 Раздел "Сводка"

О разделе:

Раздел содержит статистическую информацию о нарушениях/нарушителях.

Информация отображается на виджетах, которые располагаются на панелях (вкладках).



В разделе содержатся следующие элементы:

Элемент	Назначение
Виджеты сводки	Содержит информацию по нарушениям/нарушителям
Панели	Содержит виджеты
Кнопка  **Добавить панель**	Добавление панели

Элемент	Назначение
Кнопка **Выбрать вид**	Позволяет выбрать способ разделения рабочей области, при котором панели будут отображаться в удобных пользователю пропорциях. Возможные варианты: - деление на 3 равные части; - деление в отношении 2:1; - деление на 2 равные части; - деление в отношении 1:2.
Кнопка **Добавить виджет**	Добавление виджета
Кнопка **Выгрузить**	Выгрузка сводки о нарушениях/нарушителях (см. "Выгрузка сводки" - о параметрах выгрузки, и "Создание выгрузки" - о действиях, необходимых для формирования выгрузки)
Кнопка  **Посмотреть список выгрузок**	Просмотр созданных выгрузок

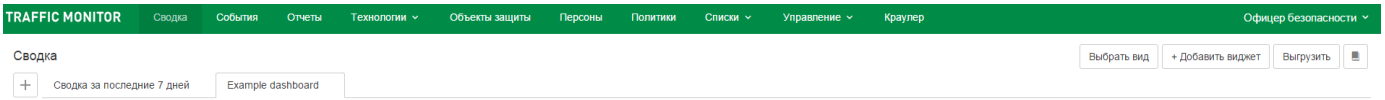
Целевые действия пользователя:

- настройка панелей и виджетов для отображения информации о нарушениях/нарушителях (см. "Создание панели" и "Создание виджета");
- просмотр информации о нарушениях/нарушителях (см. "Просмотр событий");
- составление выгрузки сводки (см. "Работа с выгрузками").

4.1.1 Панели

Рабочая область раздела **Сводка** содержит одну или несколько **панелей**: вкладок, где располагают виджеты, с помощью которых можно просматривать статистику по нарушениям и нарушителям.

Панели позволяют эргономично использовать рабочую область раздела **Сводка**.



Раздел **Сводка**, панель **Example dashboard**

Атрибуты панели описаны в таблице:

Параметр	Описание
Название	Наименование панели
Вид	Способ отображения данных на панели

Параметр	Описание
Набор виджетов	Виджеты, закрепленные на панели

Целевые действия пользователя:

- создание и настройка панели для отображения информации о нарушениях/нарушителях (см. "Создание панели" и "Создание виджета")

4.1.2 Виджеты сводки

Рабочая область раздела **Сводка** содержит панели, предназначенные для отображения виджетов.

Виджеты содержат статистическую информацию по нарушениям/нарушителям; внешний вид и параметры работы виждета определяются его типом.

Назначение различных типов виджетов и ссылки на их подробное описание приведены в таблице:

Виджет	Описание
Динамика нарушений	Количественные изменения по выбранным типам нарушений за выбранный период времени
Топ нарушителей	Список наиболее отличившихся нарушителей по выбранной группе за выбранный период времени
Количество нарушений за период	Для каждого из типа нарушений (передачи, размещения, копирования на съемные носители) отображается количество нарушений высокого, среднего, низкого уровня за выбранный период времени
Подборка	События для выбранной подборки (по выбранному фильтру)
Динамика статусов	Динамика статусов за выбранный период времени
Статистика по политикам	Количество нарушений по политикам в разрезе правил передачи, копирования и хранения за выбранный период времени
Статистика по объектам защиты	Количество нарушений по объектам защиты в разрезе уровней нарушений за выбранный период времени
Статистика по каталогам объектов защиты	Количество нарушений по каталогам объектов защиты в разрезе уровней нарушений за выбранный период времени

Целевые действия пользователя:

- настройка виджетов для отображения информации о нарушениях/нарушителях (см. "Настройка виджета")
- перемещение плиток виджетов (см. "Создание виджета")

4.1.2.1 Динамика нарушений за период

Виджет **Динамика нарушений** отображает количественные изменения по выбранным типам нарушений за выбранный период времени. Данные на виджете сгруппированы по дням.



Нарушения высокого, среднего и низкого уровня представлены на отдельных графиках. При наведении курсора на график в точках пересечения времени и количества нарушений отображаются маркеры. При нажатии на маркер выполняется переход в раздел "События", где будут показаны нарушения за выбранный день, с выбранным уровнем нарушений и типом правил.

Параметры виджета:

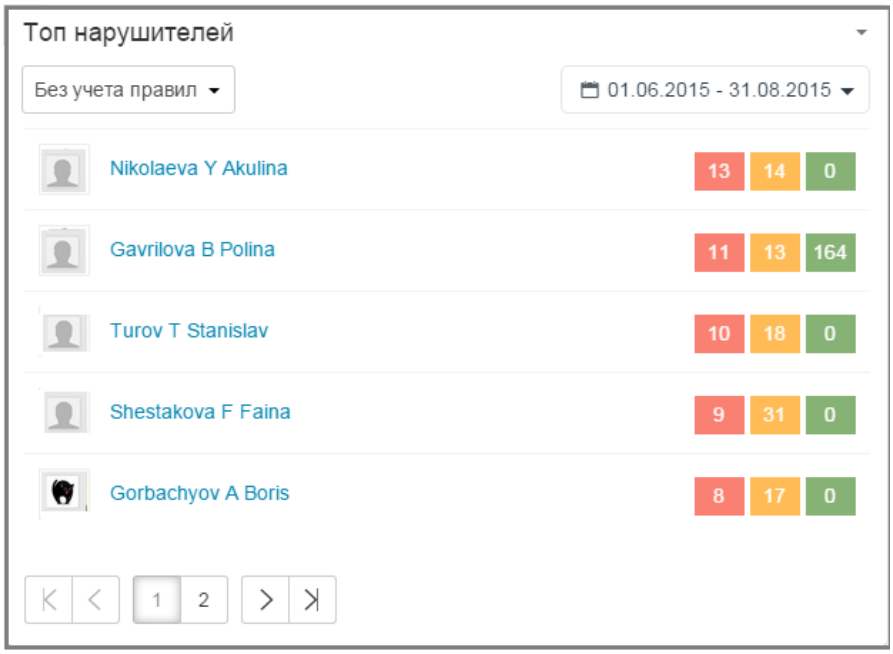
Параметр	**Описание**
Название	Название виджета
Правила	В раскрывающемся списке в верхнем левом углу виджета выберите, нарушения каких правил будут отображаются на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.

Примечание.

Чтобы изменить название виджета и выбрать интервал обновления, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.2.2 Топ нарушителей

Виджет **Топ нарушителей** отображает список наиболее активных нарушителей в разрезе количества нарушений высокого, среднего и низкого уровня за выбранный период времени.



При нажатии на количество нарушений выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в настройках виджета условиям.

При нажатии на имя нарушителя раскрывается карточка персоны (если персона была проидентифицирована; подробнее см, "Идентификация контактов в событии"). Для просмотра подробной информации о нарушителе в разделе "Персоны" нажмите на ссылку "Перейти к персоне". Для нарушителей, которые не были проидентифицированы, отображается контакт отправителя.

Атрибуты виджета:

Параметр	Описание
Название	Название виджета
Правила	В раскрывающемся списке в верхнем левом углу виджета выберите, нарушения каких правил будут отображаются на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.
Количество нарушителей	Количество нарушителей, статистика по которым будет отображаться.
Группы	Группы, в которые могут входить нарушители. Статистика по выбранным группам будет отображаться на виджете. Начните вводить название группы или нажмите + и выберите требуемые группы из списка.
Статусы	Статусы персон, информация по которым будет отображаться. Начните вводить название статуса или нажмите + и выберите требуемые статусы из списка.

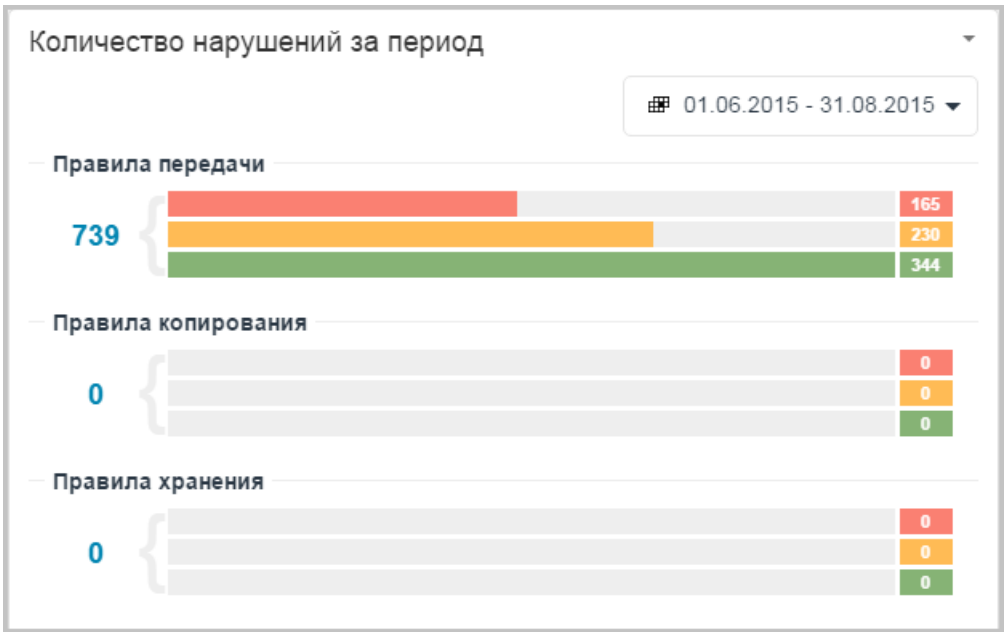
Примечание.

Чтобы изменить название виджета, выбрать интервал обновления, группы и статусы и указать количество нарушителей, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.2.3 Количество нарушений за период

Виджет **Количество нарушений за период** отображает количество нарушений высокого, среднего и низкого уровня для каждого типа правил (передачи, размещения, копирования) за выбранный период времени.

При нажатии на число, обозначающее общее количество нарушений для выбранного типа правил (выделено синим цветом), выполняется переход в раздел "События", где будут показаны нарушения за выбранный период для выбранного типа правил.



Параметры виджета:

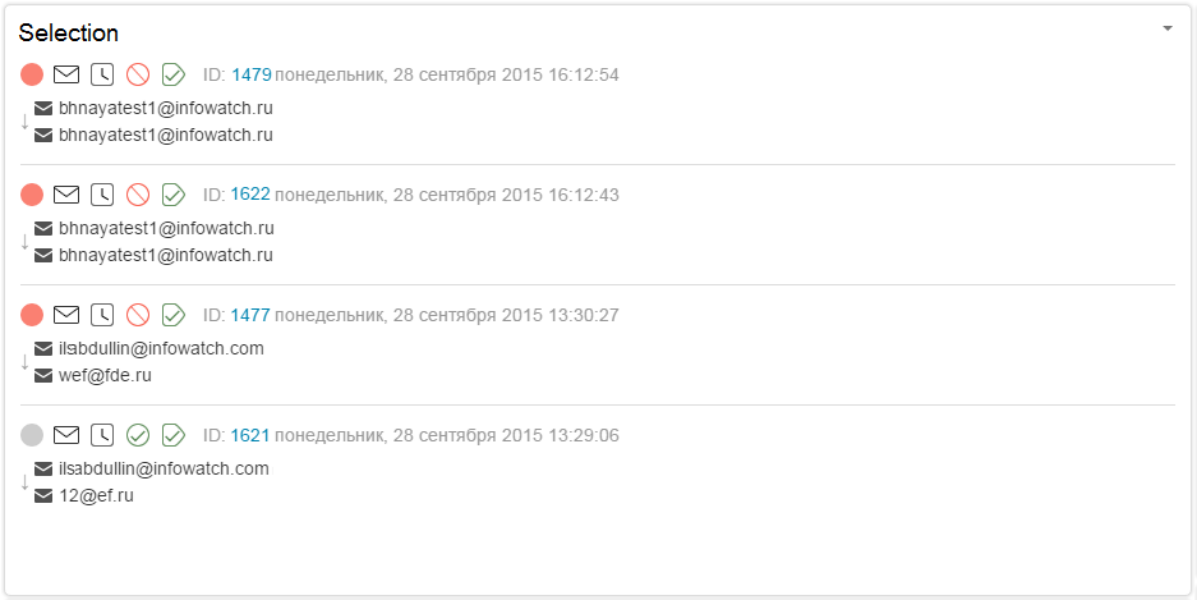
Параметр	Описание
Название	Название виджета
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.
Тип предоставления	Способ отображения данных на виджете. Возможные значения: *Столбчатая диаграмма (горизонтальная)* и *Таблица*.

Примечание:

Чтобы изменить название виджета, выбрать интервал обновления и тип представления данных, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.2.4 Подборка

Виджет **Подборка** отображает события, удовлетворяющие условиям выбранного запроса.



При нажатии на **ID** события (выделен синим цветом) выполняется переход в раздел "**События**", к краткой форме просмотра выбранного события.

Чтобы изменить атрибуты виджета, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

Атрибуты виджета:

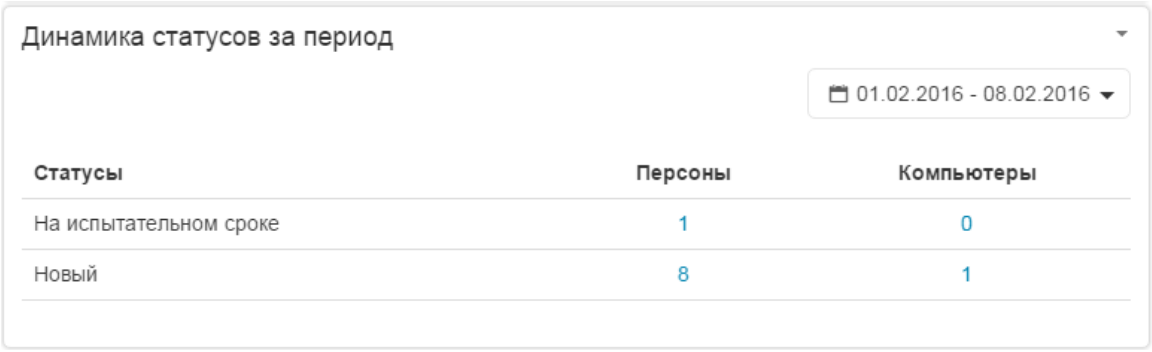
Параметр	Описание
Название	Название виджета
Интервал обновления	Периодичность обновления данных на виджете
Подборка	Запрос, по которому будет осуществляться подборка. Выберите требуемый запрос из раскрывающегося списка (подробнее см. "Запросы")
Событий на странице	Количество событий, которое будет отображаться на странице

Примечание.

При генерации выгрузки сводки (см. "Выгрузка сводки") данные виджета **Подборка** не отображаются.

4.1.2.5 Динамика статусов за период

Виджет **Динамика статусов за период** отображает изменения статусов персон за выбранный промежуток времени.



При нажатии на количество персон или компьютеров (выделено синим цветом), выполняется переход в раздел "Персоны" (к вкладке **Персоны** или **Компьютеры** соответственно), где будут показаны персоны (или компьютеры), удовлетворяющие заданным в виджете условиям.

Атрибуты виджета:

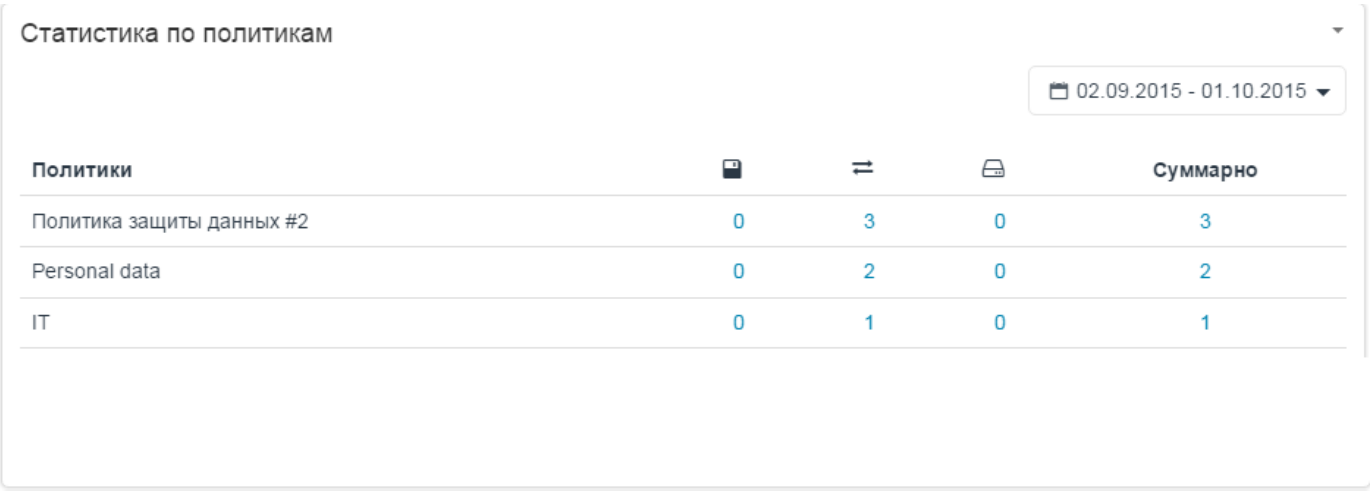
Параметр	Описание
Название	Наименование виджета
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.

Примечание:

Чтобы изменить название виджета и выбрать интервал обновления, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.2.6 Статистика по политикам

Виджет **Статистика по политикам** отображает количество нарушений по политикам в разрезе правил передачи, копирования и хранения за выбранный период времени.



При нажатии на число нарушений правил копирования, передачи, размещения (выделено синим цветом), выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в виджете условиям.

Атрибуты виджета:

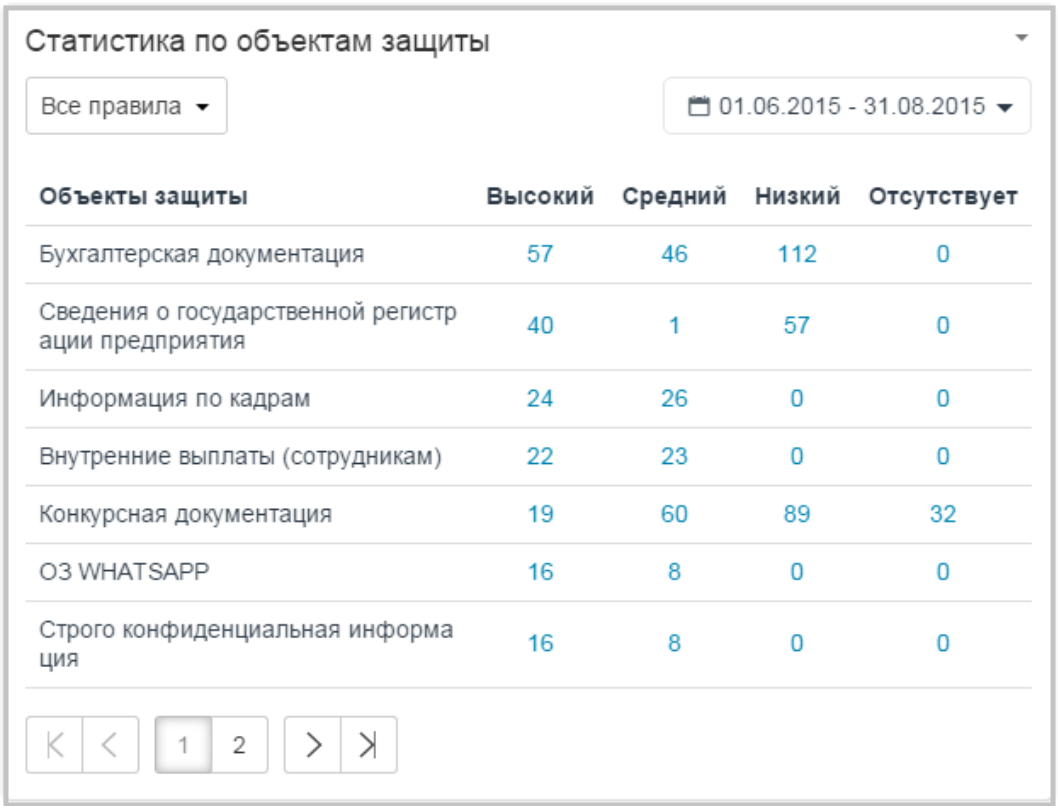
Параметр	Описание
Название	Название виджета
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.
Политики	Политики, статистика по которым будет отображаться. Начните вводить название политики или нажмите + и выберите нужные политики из списка.

Примечание:

Чтобы изменить название виджета, выбрать интервал обновления и политики, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.2.7 Статистика по объектам защиты

Виджет **Статистика по объектам защиты** отображает количество нарушений по объектам защиты в разрезе уровней нарушений за выбранный период времени.



Событие отображается в статистике, если в событии присутствует какой-либо из выбранных объектов защиты или какой-либо объект защиты из выбранных каталогов, в том числе вложенных.

При нажатии на число нарушений для каждого из объектов защиты (выделено синим цветом), выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в настройках виджета условиям.

Атрибуты виджета:

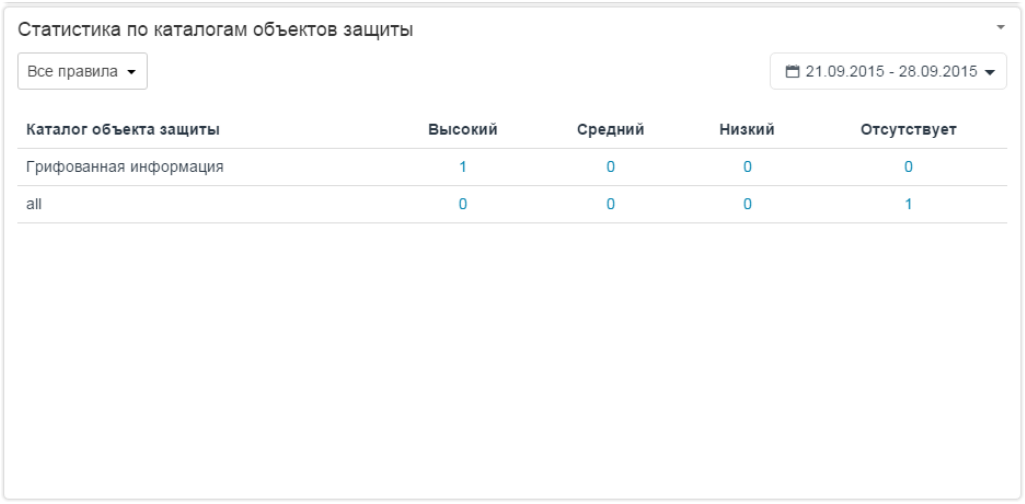
Параметр	Описание
Название	Назние виджета
Правила	В раскрывающемся списке в верхнем левом углу виджета выберите, нарушения каких правил будут отображаются на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.
Объект защиты	Объекты защиты, по которым будет отображаться статистика. Начните вводить название объекта защиты или нажмите + и выберите требуемые объекты из списка.
Каталог объекта защиты	Каталоги объектов защиты, по которым будет отображаться статистика. Начните вводить название каталога или нажмите + и выберите требуемые каталоги из списка.

Примечание:

Чтобы изменить название виджета, выбрать интервал обновления, объекты защиты и их каталоги, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.2.8 Статистика по каталогам объектов защиты

Виджет **Статистика по каталогам объектов защиты** отображает количество нарушений по каталогам объектов защиты в разрезе уровней нарушений за выбранный период времени.



Событие отображается в статистике по выбранному каталогу, если в событии присутствукт какой-либо объект защиты из этого каталога. Наличие объектов защиты из вложенных каталогов не учитывается.

При нажатии на число нарушений для каждого из каталогов объектов защиты (выделено синим цветом) выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в виджете условиям.

Атрибуты виджета:

Параметр	Описание
Название	Название виджета
Правила	В раскрывающемся списке в верхнем левом углу виджета выберите, нарушения каких правил будут отображаются на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.
Интервал обновления	Периодичность обновления данных на виджете
Период	В раскрывающемся списке в верхнем правом углу виджета укажите временной промежуток, за который выводятся данные.

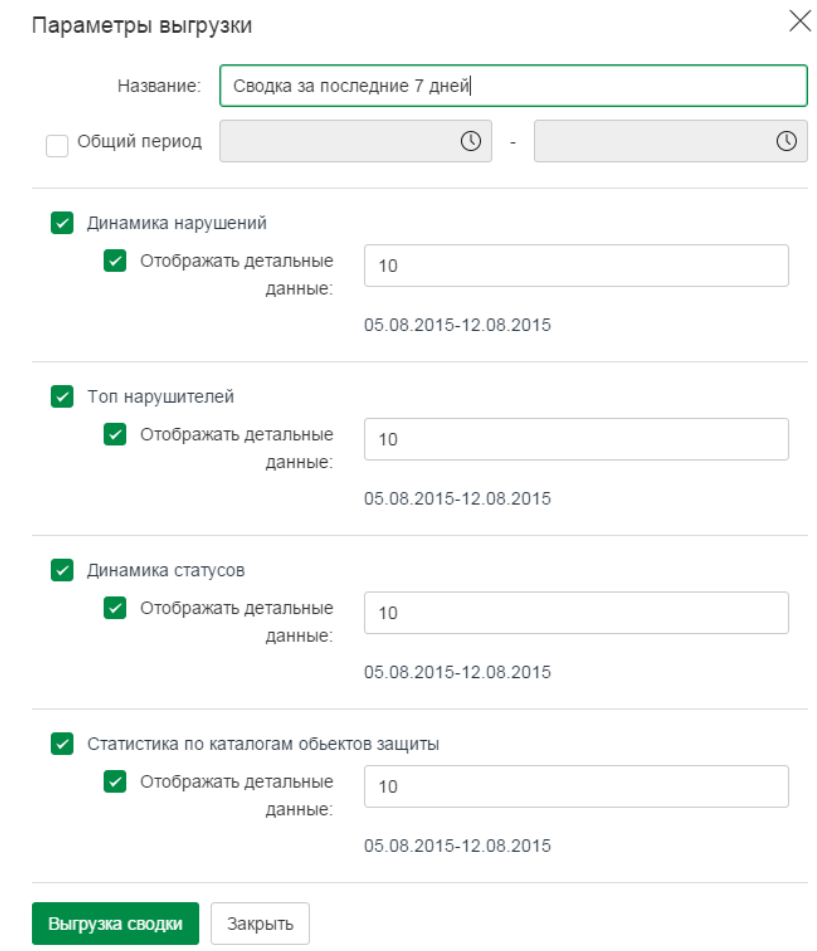
Параметр	Описание
Каталог объектов защиты	Каталог объектов защиты, сводка по которому будет отображаться. Начните вводить название каталога или нажмите + и выберите требуемые каталоги из списка.

Примечание:

Чтобы изменить название виджета, выбрать интервал обновления и каталоги объектов защиты, в верхнем правом углу виджета нажмите ▾ и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

4.1.3 Выгрузка сводки

Выгрузка сводки требуется для наглядного отображения статистических данных о перехваченных объектах, и может быть представлена в формате PDF или HTML. Вы также можете распечатать ее на принтере.



Атрибуты выгрузки:

Параметр	Описание
Название	Название выгрузки
Общий период	Отметьте эту настройку, если требуется сформировать сводку для всех виджетов за общий период. Укажите начальную и конечную дату. **Примечание.** По умолчанию сводка для каждого виджета генерируется за период, указанный в настройках виджета.
Блок виджета	Показатель того, включены ли данные виджета в выгрузку. По умолчанию выгрузка формируется для всех виджетов панели. Если вы не хотите включать данные какого-либо виджета, снимите флажок напротив его названия. **Важно!** Данные виджета "Подборка" в сводке не отображаются.
Отображать детальные данные	Отметьте эту настройку, если хотите, чтобы в выгрузке отображались отдельные объекты. При необходимости измените количество объектов, которые будут отображать в выгрузке (по умолчанию отображается 10 объектов). Например, для виджета "Динамика статусов за период" данный параметр опредяет, сколько персон персон и компьютеров для каждого статуса будут добавлены в выгрузку.

Целевые действия пользователя:

- составление выгрузки сводки (см. "Работа с выгрузками")

4.2 Раздел "События"

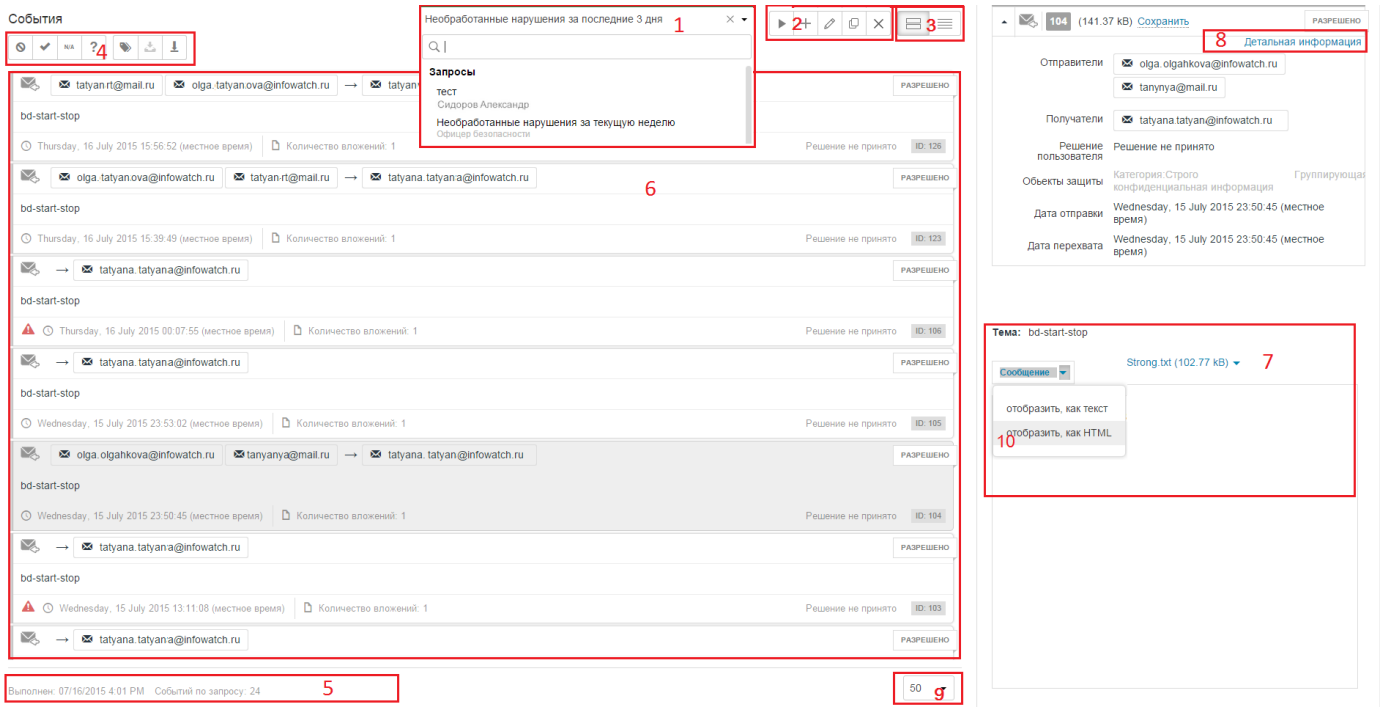
Справочная информация:
Событие - объект перехвата сетевого трафика.

События создаются Системой в результате перехвата трафика при:

- передаче данных сотрудниками другим людям;
- публикации данных в общедоступных источниках;
- копировании данных на внешние устройства;
- печати данных.

О разделе:

Раздел содержит список событий (объектов перехвата) и средства для работы с ними.
В Системе может содержаться большое число событий, поэтому список событий отображается по результатам применения пользовательских запросов.



В разделе содержатся следующие элементы:

Номер на схеме	Элемент	Назначение
1	Раскрывающийся список запросов	Содержит список доступных запросов, с помощью которых может быть произведена фильтрация объектов перехвата (см. "Запросы") **Примечание:** для каждого запроса в списке указано его название и пользователь, создавший запрос
2	Панель инструментов для работы с запросами	Набор инструментов для работы с запросами
3	Кнопки выбора стиля отображения событий	Переключение между способами отображения событий:  - отображение событий в виде плиток;  - отображение событий в виде таблицы.
4	Панель инструментов для событий	Набор инструментов для работы с событиями
5	Атрибуты события: время выполнения и количество найденных событий	Отображается дата выполнения запроса в формате MM/DD/YY, время выполнения и количество найденных событий
6	Список событий	Список объектов перехвата, найденных в результате выполнения запроса (см. "Объекты перехвата"). **Примечание:** О характеристиках плитки события см. "Плитка события"

Номер на схеме	Элемент	Назначение
7	Краткая форма просмотра события (см. "Краткая форма просмотра событий")	Набор наиболее часто используемых сведений о событии (см. "Краткая форма просмотра событий")
8	Детальная информация по событию (см. "Детальная форма просмотра событий")	Полный набор сведений о событии
9	Число отображаемых записей - раскрывающийся список	Позволяет выбрать количество событий, отображающихся на странице
10	Режим просмотра сообщения (только для писем, содержащих HTML-разметку)	Позволяет выбрать режим просмотра сообщения. Возможные значения: **отобразить как текст** - служит для отображения текста письма без форматирования. Позволяет увидеть скрытый текст (например, текст белого цвета или текст, содержащийся в названии картинки; **отобразить как HTML** - позволяет просмотреть картинки, таблицы и разметку текста.

Целевые действия пользователя:

- фильтрация событий (см. "Создание запросов");
- просмотр информации по событию ("Просмотр краткой формы события" и "Просмотр детальной формы события");
- вынесение решения по событию (см. "Вынесение решения по объекту");
- добавление/удаление тега события (см. "Добавление/удаление тега");
- сохранение события (см. "Сохранение события (для SMTP-писем)");
- досылка заблокированного события (см. "Досылка события, находящегося в карантине");
- выгрузка событий (см. "Выгрузка события");
- просмотр контактов отправителей и получателей в событии (см. "Идентификация контактов в событии").

4.2.1 Запросы

Объекты, проверенные Системой, сохраняются в базу данных. Чтобы просмотреть в Консоли управления информацию по объектам, загруженным в БД, нужно создать и применить запрос.

Запрос - это выборка объектов перехвата по заданным условиям.

Предусмотрено два режима создания запроса: обычный (позволяет выбрать нужные условия из списка) и расширенный (позволяет выполнить более гибкую настройку параметров поиска).

Форма создания запроса содержит следующие вкладки:

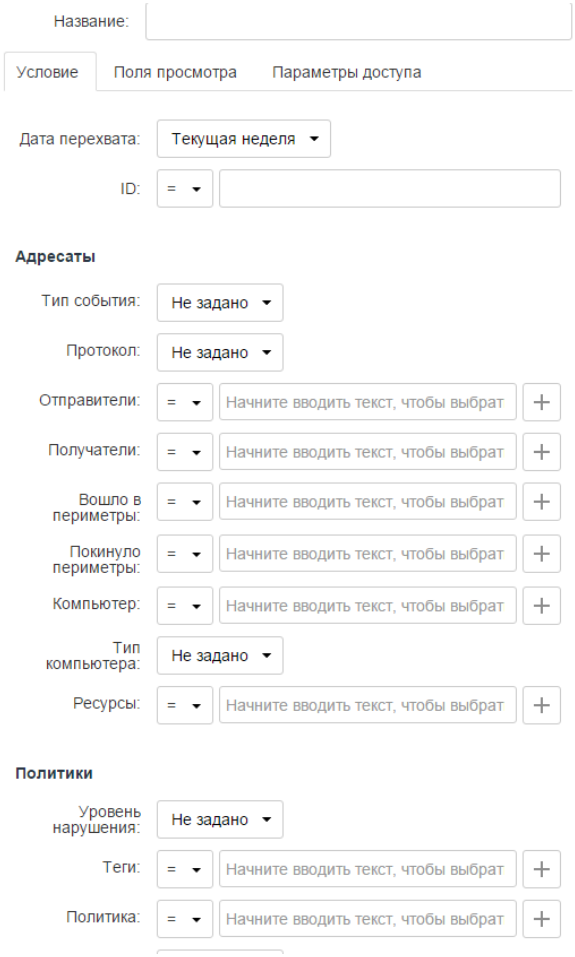
Элемент	**Назначение**

Условие	На этой вкладке вы можете указать условия, по которым будет производиться фильтрация
Поля просмотра	На этой вкладке вы можете выбрать, какие поля просмотра будут отображаться в записях событий
Параметры доступа	На этой вкладке вы можете настроить доступ только для владельца запроса

Целевые действия пользователя:

- указание параметров запроса (см. "Создание запросов");
- определение полей просмотра (см. "Выбор полей просмотра событий").

4.2.1.1 Условие



Раздел **События**, вкладка **Условие** для выбранного запроса

Атрибуты условия фильтрации:

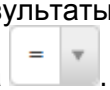
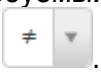
Параметр	**Описание**
=	Параметр равенства атрибуту

≠	Параметр отрицания атрибута
Дата перехвата	Дата, когда было создано событие. По умолчанию будут показаны события за текущую неделю.
ID объекта	Уникальный идентификатор события. Может быть указано несколько значений через запятую.
Тип события	Характеристика, указывающая на принадлежность события к тому или иному перехватчику. Типы событий сгруппированы по категориям. При выборе категории будут выбраны все входящие в нее типы событий. Доступные значения: • Интернет-активность: - Веб-сообщение • Обмен файлами: - FTP - Внешнее устройство • Принтеры и МФУ - Печать • Запись мультимедиа - Фотография • Размещение - Краулер • Электронная почта - Электронная почта - Веб-почта • Мессенджер - WhatsApp - Yahoo! - MS Lync - ICQ - XMPP - MMP - Skype • Сотовая связь - SMS
Протокол	Протокол, по которому осуществляется передача трафика
Отправители	Список отправителей объекта
Получатели	Список получателей объекта
Вошло в периметры	Периметр, в котором находится получатель трафика
Покинуло периметры	Периметр, в котором находится отправитель трафика
Компьютер	Компьютер, с которого был отправлен объект

Тип компьютера	Тип компьютера, с которого был отправлен объект. Возможные значения: • компьютер • мобильное устройство • терминальный сервер
Ресурсы	Интернет-ресурс или группа ресурсов (см. "Список ресурсов"). Начните вводить название ресурса или группы и выберите требуемое значение из списка подсказок, предложенных Системой. **Примечание**. При указании конкретного ресурса необходимо выбирать значение, для которого отоброжается символ  (например, ).
Уровень нарушения	Уровень нарушения политики корпоративной безопасности. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*.
Теги	Теги, присвоенные объекту (см. "Теги")
Политика	Список политик, сработавших на объекте
Тип нарушения	Тип правила, которое было нарушено. Возможные значения: *Нарушение передачи*, *Нарушение копирования*, *Нарушение хранения.*
Решение пользователя	Решение, принятое пользователем по объекту. Возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ.*
Вердикт	Вердикт, вынесенный Системой по объекту. Возможные значения: *Разрешено*, *Заблокировано*, *Карантин*.
Название задачи	Название задачи сканирования.
Дата запуска задачи	Временной период, в который задача была запущена
Цель сканирования	Тип локации, на которой объект был найден. Возможные значения: • Разделяемые сетевые ресурсы • Локальные диски рабочих станций • Файловое хранилище SharePoint
Название вложения	Название вложения, содержащегося в объекте. Указывается имя файла и его расширение.
Формат вложения	Формат вложения. Можно выбрать несколько значений из списка.
Зашифрованный файл	Применяется ли к вложению шифрование
Путь к файлу	Источник файла
Дата создания файла	Дата создания вложенного файла

Дата модификации файла	Дата изменения вложенного файла
Размер вложения	Размер вложенного файла. Можно указать минимальный или максимальный размер файла либо оба параметра.
Текст события	Укажите текст для поиска. Будут найдены события, в тексте которых присутствуют все перечисленные слова без учета регистра, морфологии, порядка следования и расположения слов. Поиск выполняет по всему содержимому события. Использование групповых символов ("*", "?") не допускается. При отрицании условия из результатов поиска будут исключены события, к тексте которых присутствуют все указанные слова. **Примечание:** В результате поиска по тексту события будут найдены только те события, которые уже были проиндексированы на момент выполнения запроса. Индексация событий выполняется каждые десять минут, однако при большой нагрузке на сервер этот интервал может увеличиться.
Результаты анализа	Элементы технологий, обнаруженные в перехваченных данных в составе сработавших объектов защиты
Объекты защиты	Список сработавших объектов защиты

При создании или редактировании условий можно задать положительные и отрицательные параметры запроса:

- Чтобы результаты запроса включали требуемый атрибут, установите напротив него параметр равенства .
- Чтобы исключить требуемый атрибут из результатов запроса, установите напротив него параметр отрицания .

Настройка равенства или отрицания доступна для следующих атрибутов:

- ID объекта;
- Отправители;
- Получатели;
- Вошло в периметры;
- Покинуло периметры;
- Рабочая станция отправителя;
- Ресурсы;
- Теги;
- Политика;
- Имя вложения;
- Формат вложения;
- Теста события;
- Результаты анализа;
- Объекты защиты.

Если отрицание применяется к атрибуту с множественными значениями, то из результатов поиска будут исключены события, содержащие указанные значения. Например, если в качестве отправителей указаны адреса `user1@example.com` и `user2@example.com`, из результатов поиска будут исключены события, в которых отправителем является `user1@example.com` или `user2@example`.

Для атрибутов **Отправители**, **Получатели**, **Компьютеры** (имя компьютера или IP-адрес), **Ресурсы**, **Название задачи**, **Название вложения** и **Путь к файлу** можно указать значение с использованием групповых символов:

- "?" - вместо одного символа;
- "*" - вместо нескольких символов.

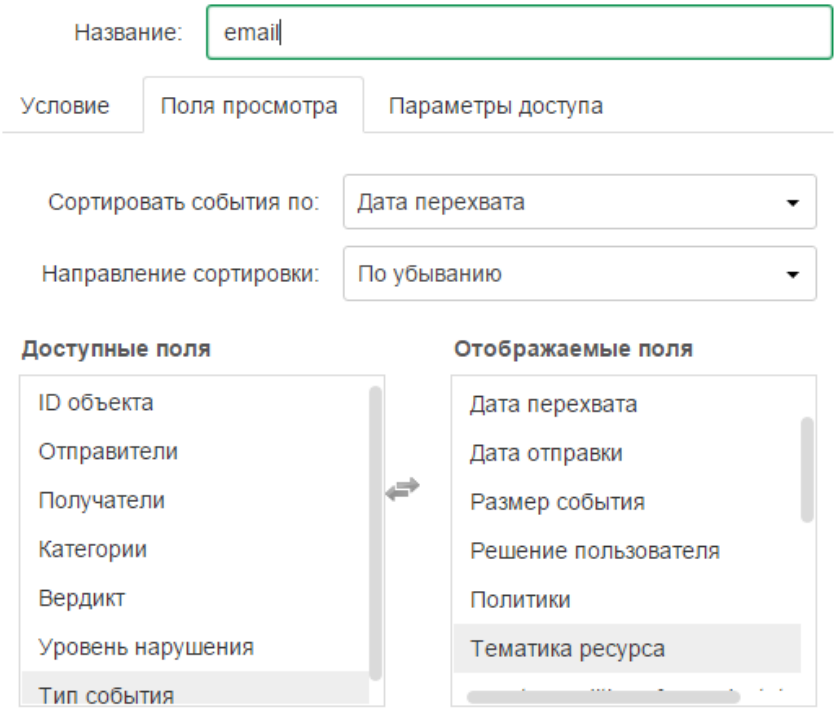
> **Примечание:**
>
> Подробнее об использовании групповых символов см. статью базы знаний "Использование в запросах групповых символов".

Целевые действия пользователя:

- Формирование стандартного запроса (см. "Создание запроса в обычном режиме")
- Формирование расширенного запроса (см. "Создание запроса в расширенном режиме")

4.2.1.2 Поля просмотра

На вкладке в левом поле представлен список доступных атрибутов события, а в правом - те атрибуты события, которые будут отображаться в табличной форме просмотра и выгружаться в файл для экспорта в формате `.xslx`. Если не выбран ни один атрибут, то в табличной форме просмотра и при выгрузке будут отображаться все атрибуты.

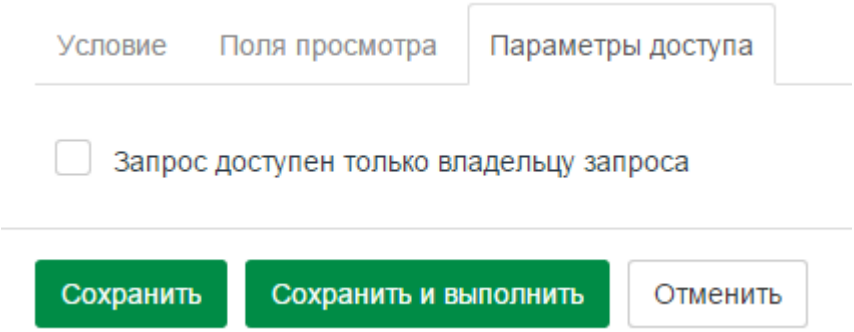


Раздел **События**, вкладка **Поля просмотра** для выбранного запроса

Целевые действия пользователя:

- Определение полей, которые будут отображаться в информации о событии (см. "Выбор полей просмотра событий")
- Выгрузка событий (см. "Выгрузка события")

4.2.1.3 Параметры доступа



Раздел **События**, вкладка **Параметры доступа** для выбранного запроса

Чтобы установить ограничение на просмотр и редактирование запроса другими пользователями:

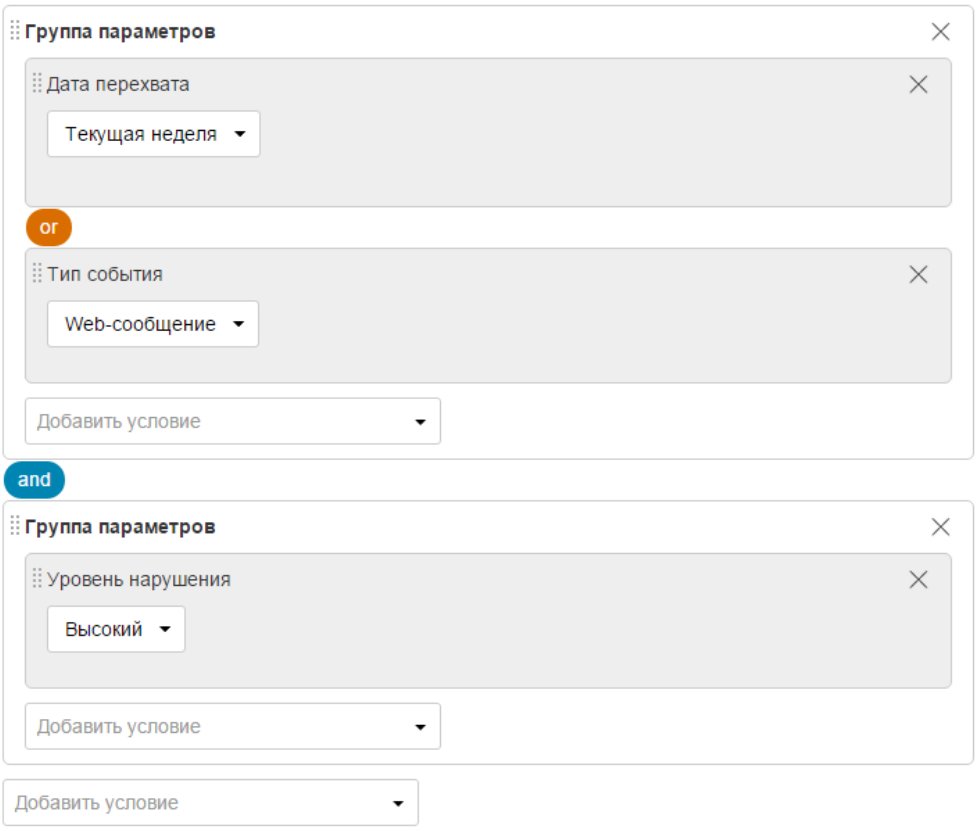
1. Установите флажок в поле **Запрос доступен только владельцу запроса**.
2. Нажмите **Сохранить**.

Чтобы открыть доступ на просмотр и редактирование запроса другими пользователями:

1. Снимите флажок в поле **Запрос доступен только владельцу запроса** (по умолчанию флажок установлен).
2. Нажмите **Сохранить**.

4.2.1.4 Расширенный режим редактирования запроса

Расширенный режим предназначен для более гибкой настройки параметров запроса.



Для составления запроса используются:

- список атрибутов событий – набор атрибутов, которые присваиваются объекту перехвата в результате анализа Системой;
- элемент *Группа параметров* – контейнер, предназначенный для логического разделения фильтра на части;
- – параметр равенства атрибуту. Индикатор того, что фильтрование событий будет учитывать наличие у события атрибутов, которым присвоен данный параметр;
-  – параметр отрицания атрибута. Индикатор того, что в результатах поиска не будут отображены те события, для атрибутов которых выставлен данный параметр.

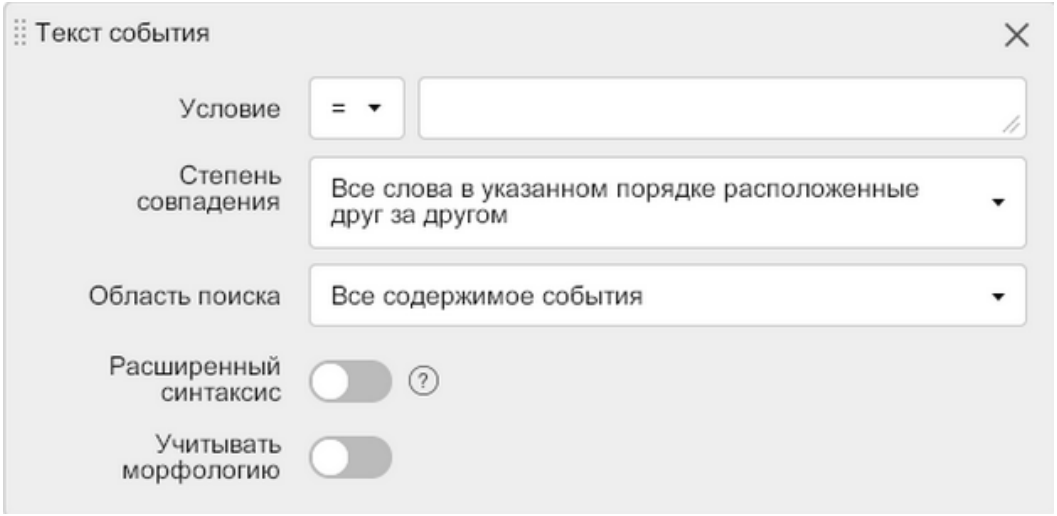
Также при создании запроса в расширенном режиме есть возможность гибкой настройки условий поиска по тексту события.

Целевые действия пользователя:

- Настройка расширенного запроса (см. "Создание запроса в расширенном режиме")

4.2.1.5 Поиск по тексту события

При создании запроса в расширенном режиме Вы можете указать условия поиска по тексту события.



Параметры полнотекстового поиска:

Параметр	Описание
Условие	Параметр равенства атрибуту. Может принимать значения: = - индикатор того, что при фильтрации событий будет учитываться наличие атрибутов, которым присвоен данный параметр; ≠ - индикатор того, что из результатов поиска будут исключены события, для атрибутов которых выставлен данный параметр.
Степень совпадения	Укажите требуемую степень совпадения: • **Все слова в указанном порядке, расположенные друг за другом** - будут найдены события, в тексте которых все перечисленные слова присутствуют в заданном порядке. При отрицании условия будут найдены события, в тексте которых отсутствуют перечисленные слова в заданном порядке. • **Все слова без учета порядка, но следующие друг за другом** - будут найдены события, в тексте которых все перечисленные слова расположены одно за другим в произвольном порядке. При отрицании условия будут найдены события, в тексте которых отсутствуют перечисленные слова в произвольном порядке. • **Все слова без учета порядка следования и расстояния между ними** - будут найдены события, в тексте которых присутствуют все перечисленные слова без учета порядка их следования и расстояния между ними. При отрицании условия будут найдены события, не содержащие перечисленные слова либо содержащее не все перечисленные слова. • **Хотя бы одно из указанных слов** - будут найдены события, в тексте которых присутствует хотя бы одно из указанных слов. При отрицании условия будут найдены события, в тексте которых не содержится ни одно из указанных слов.

Параметр	Описание
Область поиска	Укажите область, в которой будет выполняться поиск: • **Все содержимое события** - поиск будет выполняться по всему содержимому события. • **Текст сообщения** - поиск будет выполняться по тексту сообщения и теме письма. • **Тема письма** - поиск будет выполняться по теме письма. • **Вложение** - поиск будет выполняться по тексту вложений и именам файлов вложений. • **Имя файла** - поиск будет выполняться по именам файлов вложений.
Расширенный синтаксис	Включите эту настройку, если Вы хотите указать слова для поиска с помощью логических операторов. Подробнее см. "Использование расширенного синтаксиса".
Учитывать морфологию	Если данная настройка отключена, то в результате поиска будут найдены события, содержащие искомые слова только в заданной грамматической форме. **Примечание:** Опция **Учитывать морфологию** доступна, только если в настройках Базы данных включено построение морфологического индекса. Подробнее об этой настройке смотрите документ *«Руководство администратора».*

Особенности задания условий для поиска:

- в качестве разделителя между словами используется пробел;
- регистр при поиске не учитывается;
- использование групповых символов ("*", "?") не допускается.

Примечание:

В результате поиска по тексту события будут найдены только те события, которые уже были проиндексированы на момент выполнения запроса. Индексация событий выполняется каждые десять минут, однако при большой нагрузке на сервер этот интервал может увеличиться.

Важно!

В случае использования для хранения событий базы данных Oracle (см. "InfoWatch Traffic Monitor. Руководство администратора", статья "Oracle"), события, которые содержат непечатные символы (например, смайлики), не индексируются, и, соответственно, недоступны для поиска.

Целевые действия пользователя:

- Настройка расширенного запроса (см. "Создание запроса в расширенном режиме").

4.2.2 Объекты перехвата

В списке событий отображаются события, удовлетворяющие условиям запроса.

Информация о событии представлена в следующих видах:

- в плитке события (или записи о событии в таблице) отображается основная информация о событии;
- в краткой форме просмотра события отображается наиболее часто требуемая информация;
- в детальной форме просмотра события отображается наиболее полная информация об объекте перехвата.

Атрибуты объектов перехвата:

Элемент	Описание
ID объекта	Уникальный идентификатор события в Системе
Решение пользователя	Принятое пользователем решение по событию. Возможные варианты: • *Решение не принято*; • *Нарушение*; • *Нет нарушения*; • *Требуется дополнительная обработка*.
Тип события	Характер действий, повлекших создание события. Возможные варианты: •  - Интернет-активность (post-запросы к веб-ресурсам); •  - Обмен файлами (копирование файлов на внешнее устройство, передача по протоколу FTP); •  - Принтер и МФУ (отправка на печать); •  - Запись мультимедиа (отправка или получение фотографий); •  - Электронная почта (отправка и получение данных по электронной и Web-почте); •  - Мессенджер (отправка или получение сообщений через Skype, Mail.Ru Agent (MMP), MS Lync, ICQ (OSCAR), XMPP, Yahoo, WhatsApp); •  - Сотовая связь (отправка или получение сообщений через SMS); •  - Хранение файлов (в файловом хранилище SharePoint 2007/2010/2013, в разделяемых сетевых ресурсах и на локальных дисках рабочих станций).
Дата отправки	Дата и время получения письма почтовым сервером (только для электронных писем)

Элемент	Описание
Отправители	Список отправителей трафика
Компьютер отправителя	Наименование компьютера, с которого был передан трафик.
Получатели	Список получателей трафика
Политики	Список политик, сработавших при анализе данного события
Категории	Список категорий, присвоенных данному событию
Объекты защиты	Список объектов защиты, сработавших для события
Элементы анализа	Список элементов анализа в составе сработавшего объекта защиты
Тематика сайта	Тип нецелевых ресурсов, посещенных сотрудником
Теги	Список тегов, присвоенных данному объекту
Дата перехвата	Дата и время, когда трафик был перехвачен Системой
Дата вставки	Дата и время, когда данное событие было сохранено в БД
Размер	Размер события (в байтах)
Уровень нарушения	Характеристика нарушения, присвоенная событию. Возможные варианты: • *Отсутствует* - обозначается на плитке серым (■) цветом; • *Высокий* - обозначается на плитке красным (■) цветом; • *Средний* - обозначается на плитке оранжевым (■) цветом; • *Низкий* - обозначается на плитке зеленым (■) цветом
Состояние доставки	Показатель того, было ли доставлено сообщение (только для SMTP-писем при работе Системы "в разрыв" см. документ "*Infowatch Traffic Monitor. Руководство по установке и настройке*"). Возможные варианты: • *Ожидание*; • *Доставлено*; • *Неудачно*; • *Попытка не удалась*; • *Заблокировано*

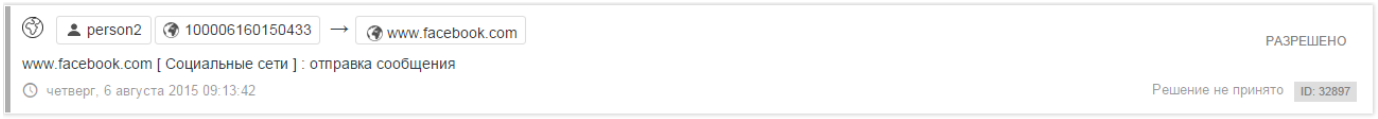
Элемент	Описание
Вердикт	Присвоенное в результате анализа Системой заключение по данному объекту. Возможные варианты: • *Разрешено* (пиктограмма) • *Заблокировано* (пиктограмма) • *Карантин* (пиктограмма)
Сервер перехвата	Имя сервера, которым был перехвачен объект.

См. также:

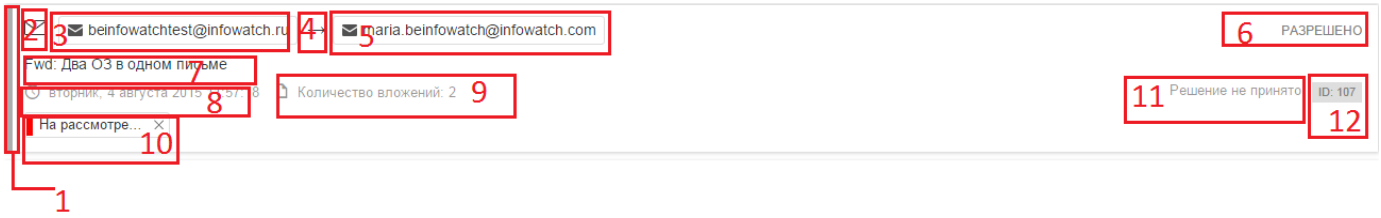
- "Плитка события" - о структуре элемента, выводящем информацию о событии по умолчанию.
- "Краткая форма просмотра событий" - о представлении общей информации о событии.
- "Детальная форма просмотра событий" - о представлении расширенной информации о событии.

4.2.2.1 Плитка события

Плитка события выглядит следующим образом:



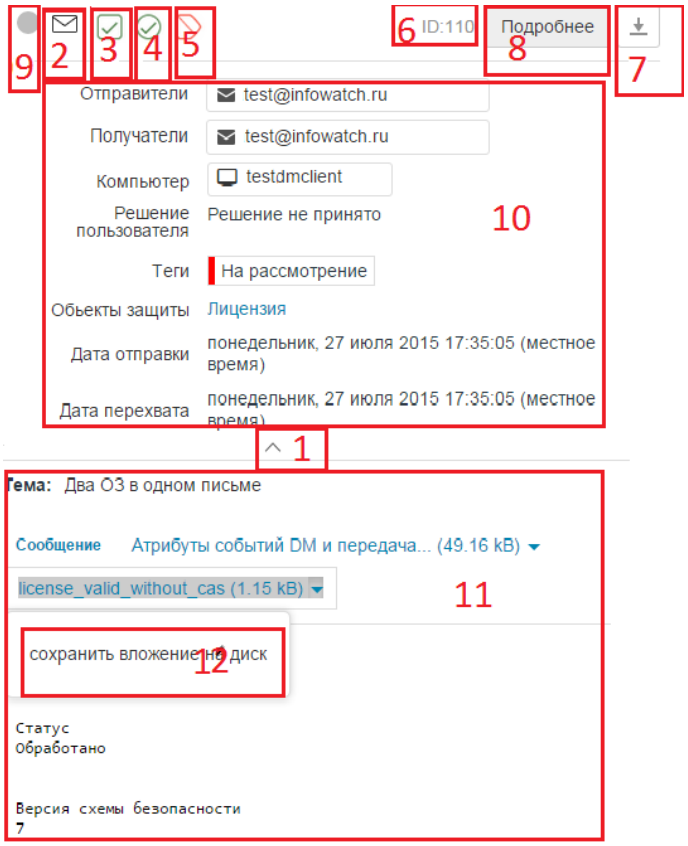
Плитка события состоит из следующих элементов:



где:
1 - Цвет уровня нарушения (возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*)
2 - Тип события. Возможные значения: *Веб-сообщение*, *FTP*, *Внешнее устройство*, *Печать*, *Фотография*, *Краулер*, *Email*, *Веб-почта*, *WhatsApp*, *Yahoo!*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3 - Отправитель (список отправителей)
4 - Направление трафика
5 - Получатель (список получателей)
6 - Вердикт (возможные значения: *Разрешено*, *Заблокировано*, *Карантин*)
7 - Превью события (краткая информация о причине возникновения события: в первом примере это отправка сообщения в социальной сети, во втором - отправка письма)
8 - Дата и время создания события
9 - Индикатор вложений
10 - Присвоенные теги (см. "Теги")

11 - Решение пользователя (возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ*)
12 - ID объекта

4.2.2.2 Краткая форма просмотра событий



Раздел **События**, краткая форма просмотра выбранного события

В краткой форме просмотра события отображаются следующие сущности:

№ на схеме	Сущность	Описание
1	Кнопка отображения/скрытия атрибутов события	Открывает или скрывает атрибуты события
2	Пиктограмма типа события	Отображает пиктограмму типа события. Возможные значения: *Веб-сообщение*, *FTP*, *Внешнее устройство*, *Печать*, *Фотография*, *Краулер*, *Email*, *Веб-почта*, *WhatsApp*, *Yahoo!*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3	Решение пользователя	Отображает значение атрибута **Решение пользователя**. Возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ*
4	Вердикт	Отображает значение атрибута **Вердикт**. Возможные значения: *Разрешено*, *Заблокировано*, *Карантин.*

№ на схеме	Сущность	Описание
5	Статус отправки	Отображает значение атрибута **Статус отправки**. Возможные значения: *Отправлено*, *Не отправлено*, *Ожидает отправки*.
6	ID объекта	Отображает значение атрибута **ID объекта**
7	Кнопка сохранения теневой копии	Кнопка, позволяющая сохранить событие на диск (см. "Сохранение события"). Отображается только для SMTP-писем.
8	Кнопка вызова детальной формы просмотра события	Открывает детальную форму просмотра события
9	Уровень нарушения	Отображает цветовое обозначение атрибута **Уровень нарушения**. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
10	Атрибуты события	Извлеченные атрибуты объекта перехвата
11	Поле просмотра события и вложений	Отображает текст события и вложения
12	Команда **Сохранить вложение на диск**	Позволяет сохранить вложения на диск компьютера

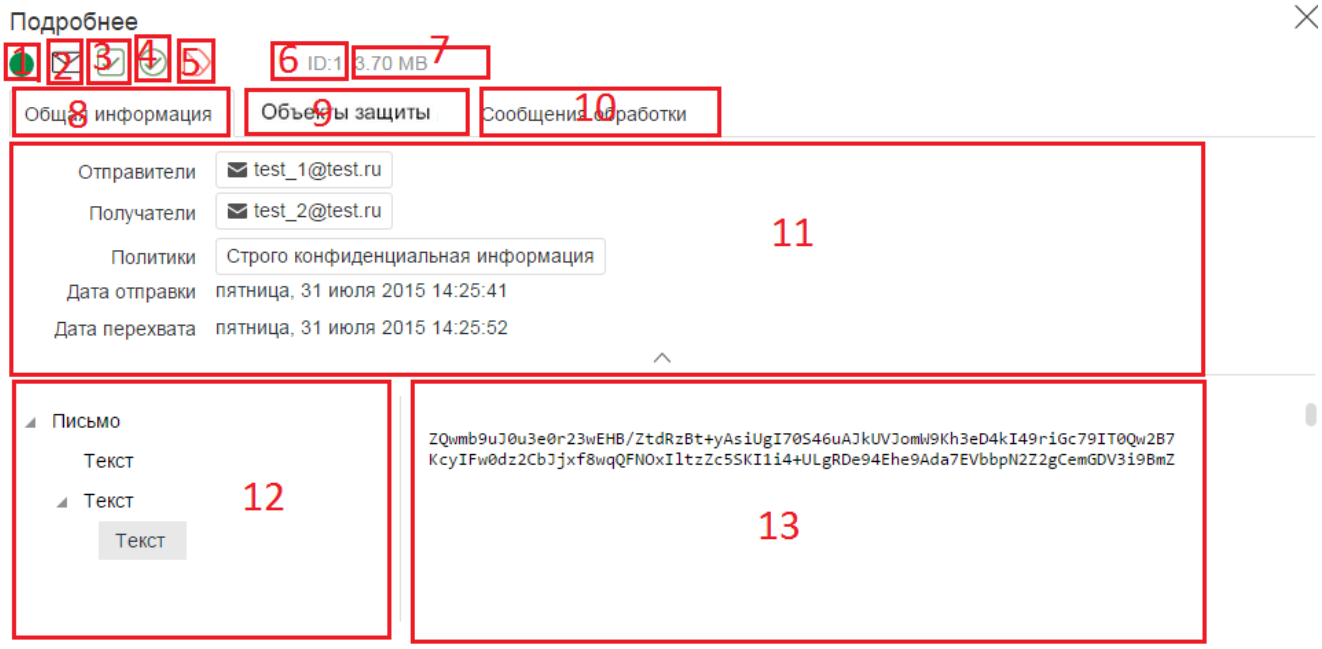
Примечание:

Набор объектов в краткой форме просмотра может различаться в зависимости от извлеченных атрибутов события.

Целевые действия пользователя:

- Ознакомление с общей информацией о событии (см. "Просмотр краткой формы события")

4.2.2.3 Детальная форма просмотра событий



Раздел **События**, детальная форма просмотра выбранного события, вкладка **Общая информация**

В детальной форме просмотра события содержатся следующие вкладки:

Вкладка	Назначение
Общая информация	Отображает общую информацию, представленную в краткой форме просмотра события
Объекты защиты	Отображает информацию о сработавших объектах защиты и входящих в них элементах анализа
Сообщения обработки	Отображает системные сообщения об этапах обработки объекта и возникших во время этого проблемах

В детальной форме просмотра события доступны следующие сущности:

№ на схеме	Сущность	Описание
1	Уровень нарушения	Отображает цветовое обозначение атрибута **Уровень нарушения**. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*.
2	Тип события	Значение атрибута **Тип события**. Возможные значения: *Веб-сообщение*, *FTP*, *Внешнее устройство*, *Печать*, *Фотография*, *Краулер*, *Email*, *Веб-почта*, *WhatsApp*,*Yahoo!*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3	Решение пользователя	Отображает значение атрибута **Решение пользователя**. Возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ*.
4	Вердикт	Отображает значение атрибута **Вердикт**. Возможные значения: *Разрешено*, *Заблокировано*, *Карантин*.

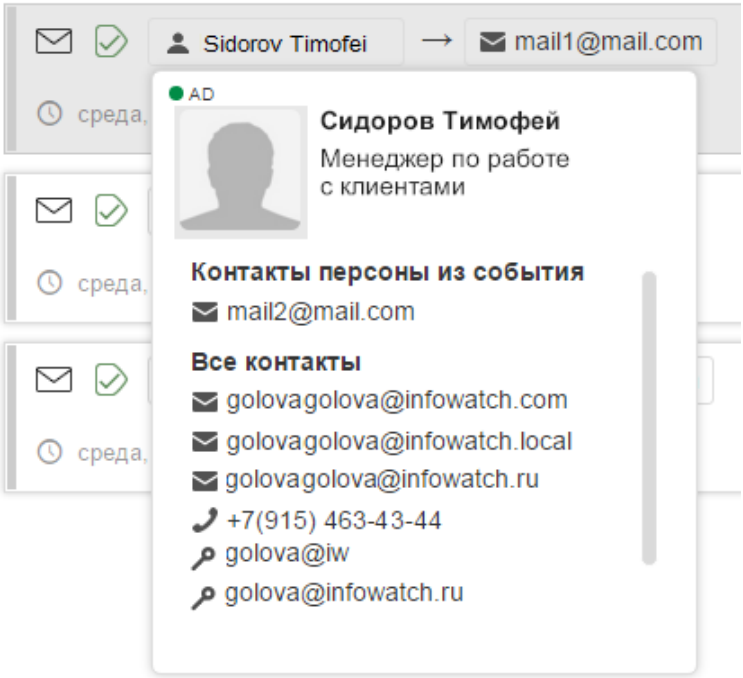
№ на схеме	Сущность	Описание
5	Статус отправки	Отображает значение атрибута **Статус отправки**. Возможные значения: *Отправлено*, *Не отправлено*, *Ожидает отправки*.
6	ID объекта	Значение атрибута **ID объекта**
7	Размер события	Значение атрибута **Размер события**
8	Вкладка **Общая информация**	Информация, представленная в краткой форме просмотра события
9	Вкладка **Объекты защиты**	Список сработавших объектов защиты и каталогов, в которых состояли данные объекты защиты на момент перехвата данных
10	Вкладка **Сообщения обработки**	Сообщения, возникшие при обработке объекта
11	Панель просмотра выбранной вкладки	Просмотр информации, в зависимости от выбранной вкладки (**Общая информация**, **Объекты защиты** или **Сообщения обработки**)
12	Панель с извлеченными атрибутами	Просмотр названий извлеченных из объекта атрибутов
13	Панель просмотра извлеченного атрибута	Просмотр извлеченных из объекта атрибутов

Целевые действия пользователя:

- Ознакомление с расширенной информацией о событии (см. "Просмотр детальной формы события")

4.2.3 Идентификация контактов в событии

На основе информации, извлеченной из события, Система определяет отправителей и получателей трафика (персон, группы персон, а также компьютеры). Этот процесс называется ***идентификацией*** контактов. Для идентифицированных отправителей и получателей на плитке события отображается имя персоны, имя компьютера или название группы, при нажатии на которое раскрывается карточка отправителя или получателя. Карточка содержит контакты, извлеченные из события, а также контактные данные, хранящиеся в Системе.



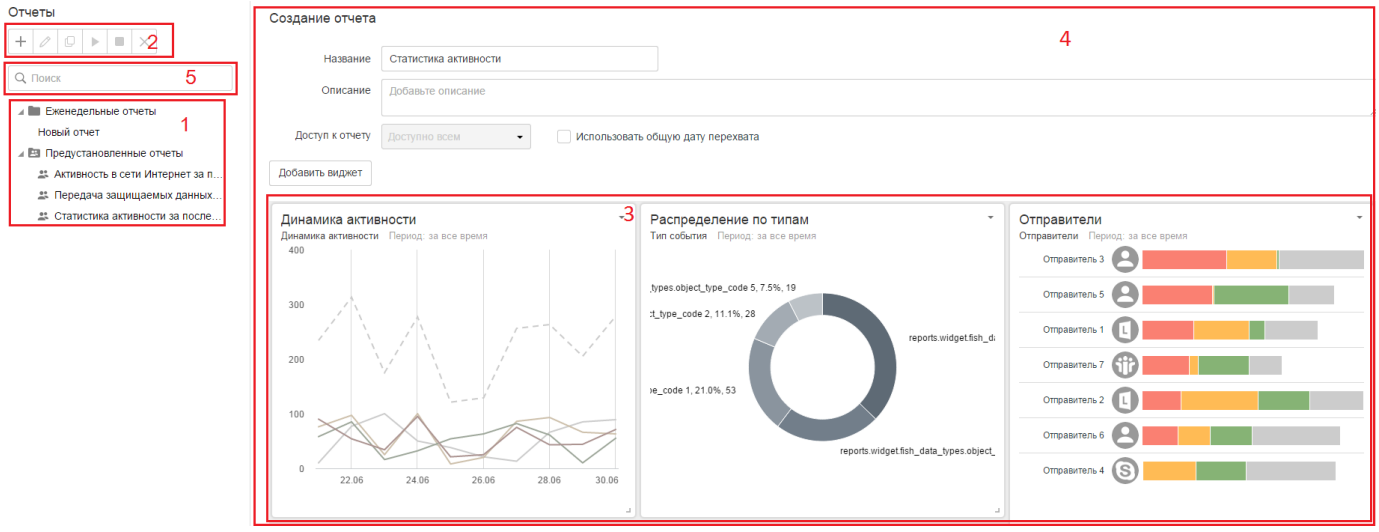
Если при обработке события Система определяет новые личные контакты персоны, найденные контакты автоматически добавляются в карточку персоны. Процесс автоматического добавление новых контактов имеющимся персонам называется ***пост-идентификацией***. В результате пост-идентификации в карточку персоны могут быть добавлены такие данные как адрес электронной почты, учетные данные мессенджеров (ICQ, Skype), мобильный телефон, а также учетные записи в социальных сетях.

4.3 Раздел "Отчеты"

О разделе:

Раздел содержит выборку статистических данных о перехваченных объектах.

Статистическая информация отображается на виджетах в виде графиков и диаграмм. Каждый отчет может содержать один или несколько виджетов.



В разделе содержатся следующие элементы:

Номер на схеме	Элемент	Назначение
1	Раскрывающийся список папок с отчетами	Содержит список папок, в которых сгруппированны доступные отчеты
2	Панель инструментов для работы с отчетами	Набор инструментов для работы с отчетами
3	Виджеты	Содержат графическое представление статистических данных о перехваченных объектах
4	Форма создания и редактирования отчета	Содержит параметры отчета и добавленные виджеты
5	Поле поиска	Поле, в котором можно ввести текст для поиска по названию папки или отчета

В папке **Предустановленные отчеты** содержатся следующие отчеты:

Отчет	Описание
Статистика активности за последние 7 дней	Показывает информацию о количестве перехваченных Системой событий, наиболее активных отправителях и получателях, а также о наиболее популярных контентных маршрутах отправителей-получателей
Активность в сети Интернет за последние 7 дней	Показывает, на какие ресурсы сети Интернет сотрудники компании наиболее часто отправляли запросы
Передача защищаемых данных за последние 7 дней	Показывает, какие объекты защиты содержались в перехваченных Системой событиях, а также какие политики информационной безопасности были применены к событиям

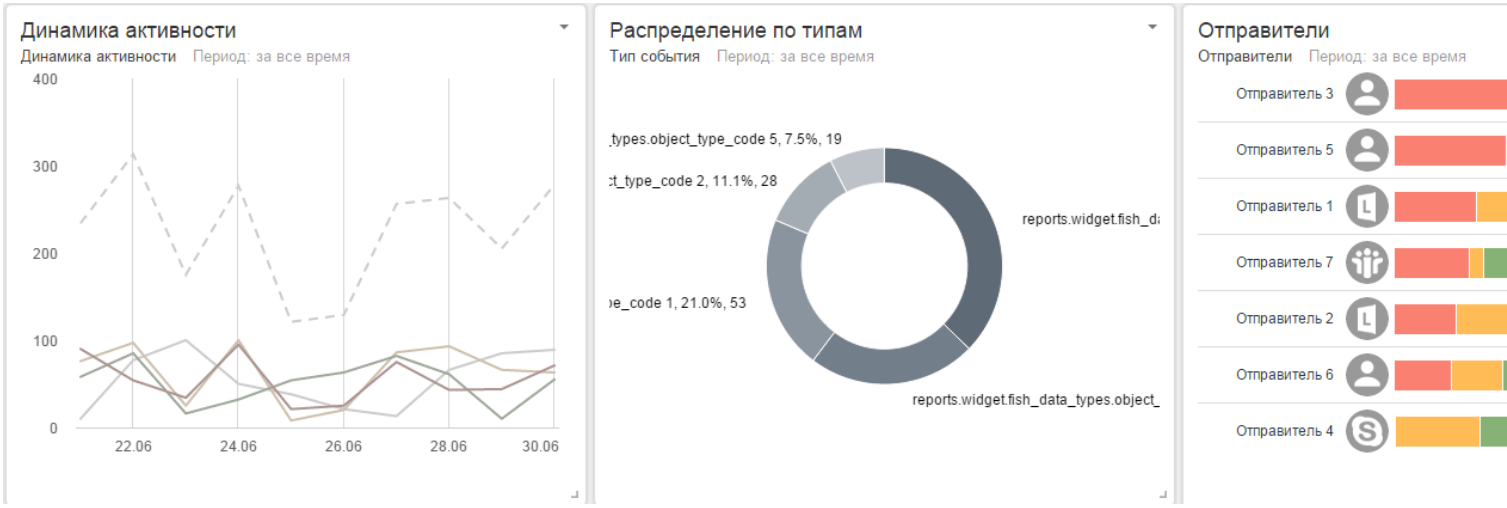
Предустановленные отчеты доступны всем пользователям Системы.

Целевые действия пользователя:

- формирование отчета;
- настройка виджетов для отображения статистической информации;
- создание папки с отчетами;
- работа с готовыми отчетами.

4.3.1 Виджеты отчетов

В правой части рабочей области раздела **Отчеты** отображаются виджеты.



Виджеты в разделе **Отчеты**

Виджеты предназначены для отображения статистической информации по перехваченным объектам за выбранный период времени.

Виджеты могут быть созданы для следующих данных:

Тип статистики	Описание
Веб-ресурсы	Веб-ресурсы, на которые сотрудники отправляли наибольшее число запросов
Диалоги	Маршруты передачи сообщений (без учёта направления), для которых Системой зафиксировано наибольшее количество событий
Динамика активности	Динамика количества событий, перехваченных Системой
Каталоги объектов защиты	Каталоги объектов защиты, наиболее часто встречающиеся в перехваченных Системой данных
Компьютеры	Компьютеры, для которых Системой зафиксировано наибольшее количество событий
Объекты защиты	Объекты защиты, наиболее часто встречающиеся в перехваченных Системой данных
Отправители	Отправители, для которых Системой зафиксировано наибольшее количество событий
Политики	Политики, наиболее часто применявшиеся к перехваченным данным
Получатели	Получатели, для которых Системой зафиксировано наибольшее количество событий
Решения пользователей	Статистика решений, принятых офицером безопасности по событиям, перехваченным Системой
Списки ресурсов	Наиболее частые тематики веб-ресурсов, на которые сотрудники отправляли запросы
Типы событий	Распределение количества событий по типам (почта, Skype, внешние устройства и т.д.)

Для выбранного типа статистики можно указать один из следующих способов отображения данных:

-  - линейчатая диаграмма с группировкой;

-  - линейчатая диаграмма с накоплением;
-  - круговая диаграмма;
-  - график.

Примечание:

Для типа статистики "Динамика активности" можно использовать только диаграмму "График". Для всех остальных типов статистики диаграмма "График" недоступна.

Параметры виджета для типа статистики "Динамика активности":

Параметр	Описание
Уровни нарушений	В виджет будут добавлены события с указанным уровнем нарушения. Установите флажки напротив требуемых значений.
Период группировки	Укажите период, за который будут сгруппированы события. Доступные значения: • минута; • час; • день; • неделя; • месяц; • квартал; • год.

Параметры виджета для остальных типов статистики:

Параметр	Описание
Тип диаграммы	Доступны следующие типы: • линейчатая диаграмма с группировкой; • линейчатая диаграмма с накоплением; • круговая диаграмма (недоступно для типа статистики "Диалоги").
Число записей	Число записей, которые будут отображаться на виджете. Укажите значение от 1 до 100. **Примечание**. Для типа статистики "Решения пользователей" данная настройка не отображается.
Объединить остальные записи в пункт "Другое"	Отметьте эту настройку, если Вы хотите, чтобы на виджет был добавлен элемент "Другое", объединяющий оставшиеся записи. **Примечание**. Для типа статистики "Решения пользователей" данная настройка не отображается.

Параметр	Описание
Показывать значения	Отметьте эту настройку, если Вы хотите, чтобы на виджете отображались количественные значения.
Показывать доли	Данная настройка доступна, если используется круговая диаграмма.

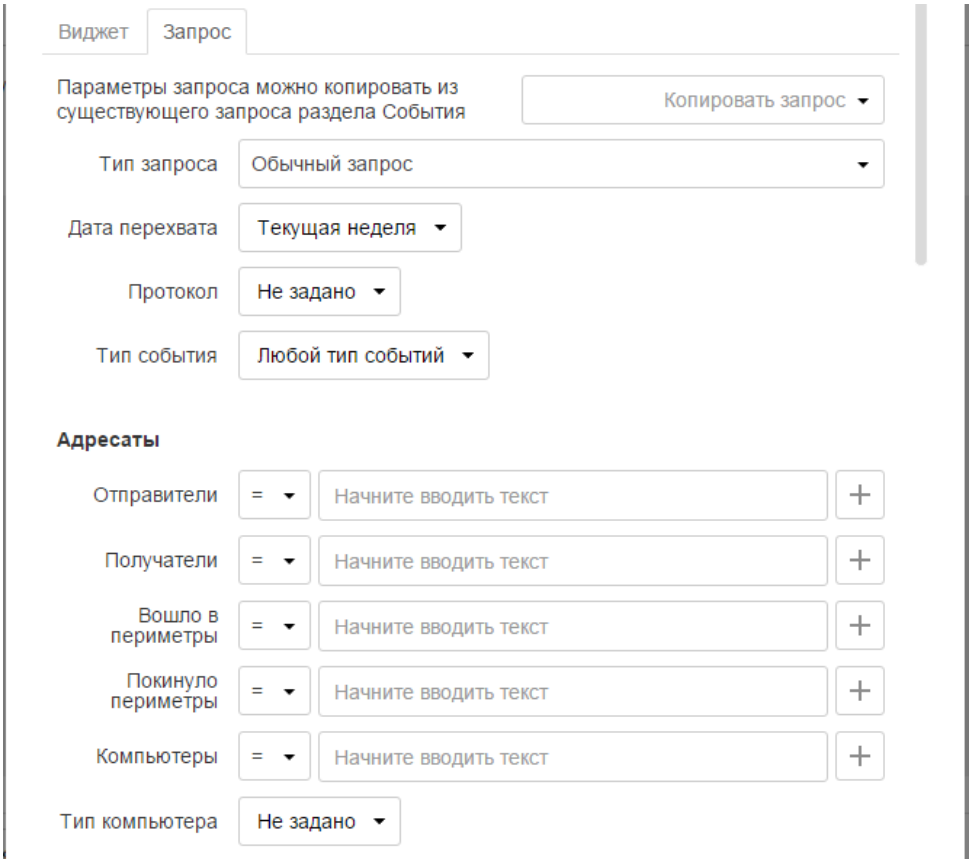
Целевые действия пользователя:

- настройка виджетов для отображения статистической информации (см. "Работа с виджетами отчетов")

4.3.2 Запросы

Запрос позволяет осуществить выборку объектов перехвата, которые будут отображаться на виджете.

Вы можете скопировать параметры запроса, добавленного в разделе **События**, либо создать новый запрос.



Вкладка **Запрос** в окне создания виджета

Запрос может быть создан в обычном либо в расширенном режиме. Обычный режим позволяет выбрать условия поиска из списка (подробнее см. "Условие").

В расширенном режиме Вы можете выполнить более гибкую настройку условий поиска (подробнее см. "Расширенный режим").

Целевые действия пользователя:

- сформировать запрос (см. "Создание запроса в стандартном режиме" и "Создание запроса в расширенном режиме").

Пример 1:

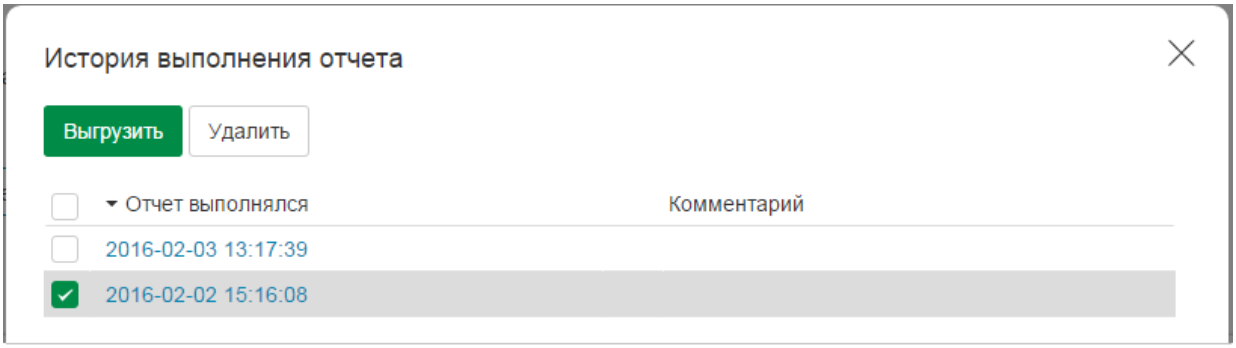
Если в запросе указать условие "Объекты защиты: IT служба ***ИЛИ*** Конкурсная деятельность ***ИЛИ*** Конфиденциальная информация", то в отчёт попадут события, в которых найдены хотя бы один из указанных ОЗ.
То есть, если в событии есть ОЗ "IT служба" и "Отдел кадров", то оба события с этими ОЗ попадут в отчёт.

Пример 2:

Если указать условие "Объекты защиты: ***НЕ*** Отдел кадров ***ИЛИ НЕ*** Персональные данные ***ИЛИ НЕ*** Финансовая информация", то из отчёта будут исключены события, в которых встречались эти ОЗ.
То есть, если было событие с ОЗ и "IT Служба", и "Отдел кадров", то это событие вообще не попадёт в статистику.

4.3.3 История выполнения отчета

История выполнения отчета позволяет просмотреть выполненные отчеты, удалить ненужные версии и сохранить выбранные версии отчета в файл.



Атрибуты истории выполнения отчета:

Параметр	Описание
Дата выполнения	Дата и время выполнения отчета
Комментарий	Комментарий к отчету, добавленный пользователем

Целевые действия пользователя:

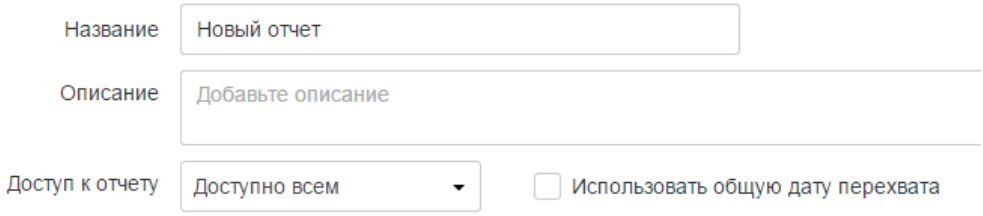
- просмотреть историю выполнения отчета, при необходимости удалить выбранные версии отчета или сохранить их в файл (подробнее см. "Работа с готовыми отчетами").

4.3.4 Форма создания отчета

Форма создания (редактирования) отчета отображается при создании нового или редактировании существующего отчета.

В левой части рабочей области раздела **Отчеты** отображается список папок, содержащих отчеты.

Отчеты позволяют сформировать статистику на основе данных, хранящихся в Системе.



Атрибуты отчета:

Параметр	Описание
Название	Название отчета
Описание	Описание в произвольной форме
Доступ к отчету	Укажите, будет ли созданный отчет доступен всем пользователям либо только владельцу. Данная опция доступна только для отчетов первого уровня. При создании отчетов внутри папки уровень доступа для отчета определяется уровнем доступа, указанным для папки.
Использовать общую дату перехвата	Установите флажок в этом поле, если Вы хотите, чтобы указанная дата перехвата использовалась для всех добавленных запросов. При выборе данной настройки появится выпадающий список, в котором Вы можете указать требуемый период.

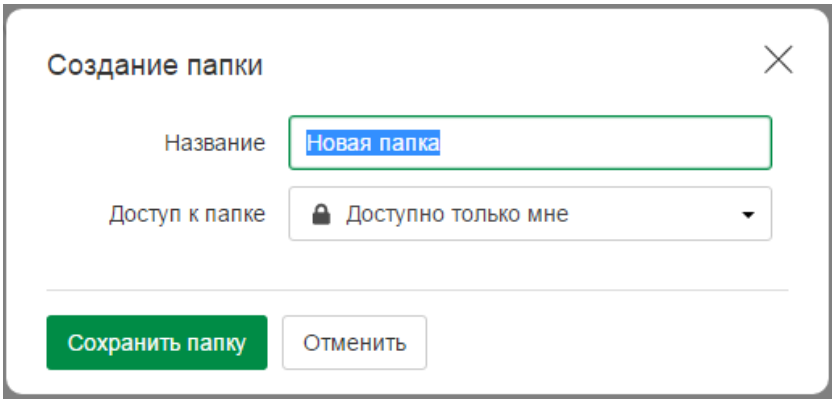
Целевые действия пользователя:

- Создание отчета

4.3.5 Форма создания папки с отчетами

В левой части рабочей области раздела **Отчеты** отображается список папок.

Папки позволяют группировать отчеты по какому-либо признаку, наследовать права доступа, а также копировать выбранную группу отчетов.



Атрибуты папки:

Параметр	Описание
Название	Название папки
Доступ к папке	Будет ли созданная папка доступна всем пользователям либо только владельцу. Данная опция доступна только для папок первого уровня. При создании вложенных папок уровень доступа наследуется от родительской папки.

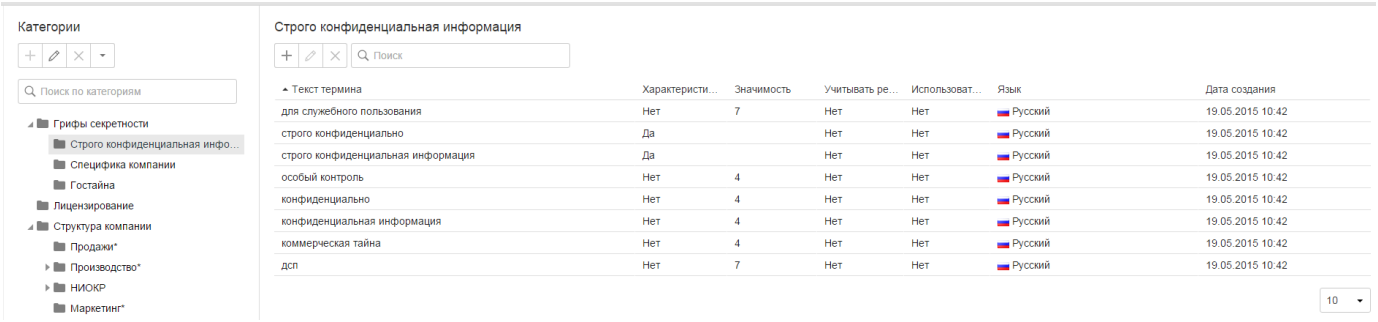
Целевые действия пользователя:

- Создание папки с отчетами

4.4 Раздел "Технологии"

Справочная информация:
Технологии представляют собой совокупность данных, используемых при анализе объектов перехвата.

О разделе:
Раздел содержит редактируемые справочники категорий и терминов, текстовых объектов, эталонных документов, бланков, печатей, выгрузок из БД, а также список предустановленных графических объектов.



Раздел **Технологии**, подраздел **Категории и термины**

В разделе содержатся следующие элементы:

Элемент	Назначение

Элемент	Назначение
Вкладки с типами справочников: • Категории и термины • Список текстовых объектов • Список эталонных документов • Список бланков • Список печатей • Список выгрузок из БД • Список графических объектов	Содержат списки элементов и инструменты для выбранного справочника
Панель инструментов	Набор инструментов для работы с выбранным справочником
Панель навигации по страницам	Набор кнопок для просмотра страниц, содержащих записи (в случае, если не все записи помещаются на одной странице)
Регулятор количества записей	Раскрывающийся список, в котором устанавливается количество записей на странице

Целевые действия пользователя:

- Формирование списка категорий и терминов (см. "Создание категорий и терминов")
- Формирование списка текстовых объектов (см. "Создание текстовых объектов и их значений")
- Формирование списка эталонных документов (см. "Создание эталонных документов")
- Формирование списка эталонных бланков (см. "Создание эталонных бланков")
- Формирование списка эталонных печатей (см. "Создание эталонных печатей")
- Формирование списка выгрузок из БД (см. "Создание эталонных выгрузок из БД")

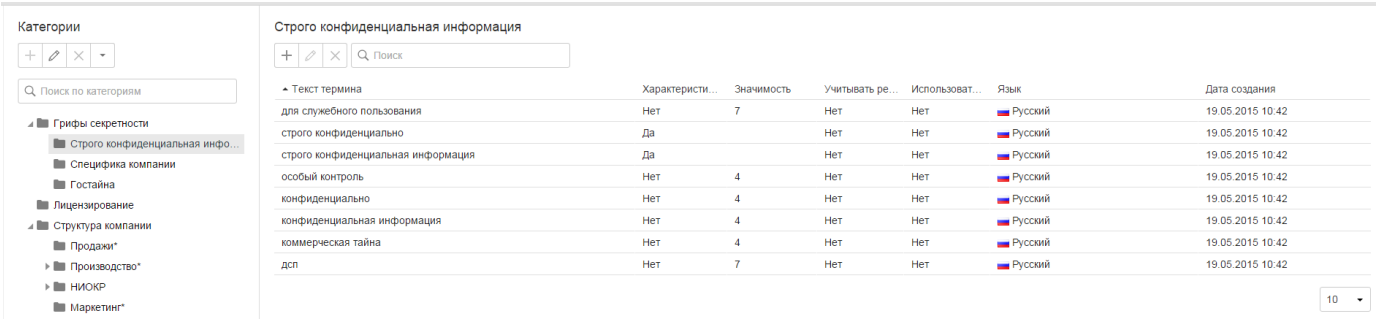
4.4.1 Категории и термины

Справочная информация:

Категории и термины - это набор данных, необходимых для проведения лингвистического анализа.

Категории классифицируют возможные нарушения политики безопасности. Наличие в тексте элемента, принадлежащего определенной категории, позволяет соотнести текст с этой категорией.

Например, категория *Финансы* содержит финансовую терминологию (*платеж*, *инвесторы*, *цены* и пр.). Таким образом, наличие в тексте терминов "платеж", "инвесторы" или "цены" позволяет соотнести текст с категорией *Финансы*.



В подразделе содержатся следующие элементы:

Параметр	Описание
Список категорий	Набор предметных областей, которым могут соответствовать перехваченные объекты
Список терминов	Набор терминов для выбранной категории
Панель инструментов	Набор инструментов для категорий и входящих в категории терминов
Строка поиска	Строка, в который Вы можете ввести текст для поиска по категориям
Панель навигации по страницам	Набор кнопок для просмотра страниц, содержащих записи (в случае, если не все записи помещаются на одной странице)
Регулятор количества записей	Раскрывающийся список, в котором устанавливается количество записей на странице

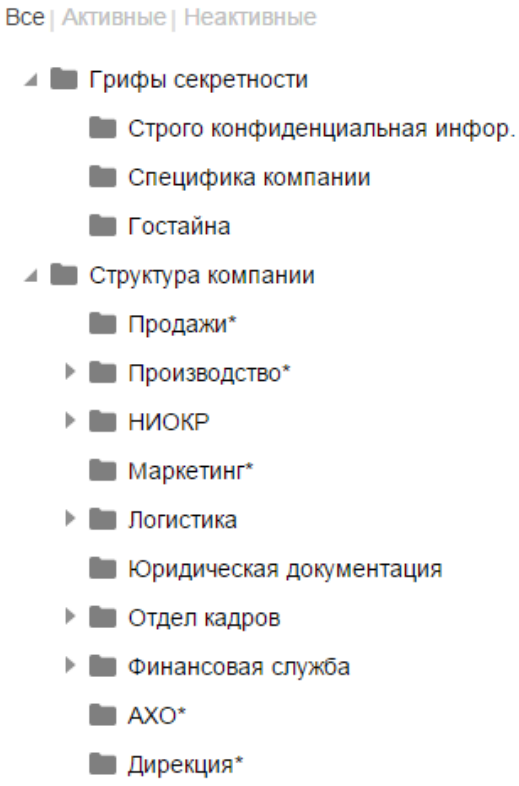
Целевые действия пользователя:

- Формирование списка категорий и терминов (см. "Создание категорий и терминов")
- Импорт и экспорт категорий и терминов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Добавление категорий в объекты защиты ("Создание объекта защиты")

4.4.1.1 Категории

Справочная информация:

Категория представляет собой набор элементов, соответствующих определённой предметной области (например, *Грифы секретности* или *Термины проекта*). Содержит либо перечень категорий (подкатегорий), либо перечень элементов, характерных для данной категории.



Примечание:

Предустановленные категории, помеченные знаком астериска (*), не содержат объектов, и заполняются на этапе внедрения Системы или позже, в рамках кастомизации.

Атрибуты категории:

Параметр	Описание
Название	Наименование категории
Вес	Значение, указываемое по умолчанию для всех терминов категории в качестве атрибута **Вес**
Язык	Язык терминов категории
Учитывать морфологию	Показатель использования морфологии при анализе траффика
Учитывать регистр	Показатель учета регистра при анализе траффика
Описание	Примечание в произвольной форме
Дата создания	Дата и время создания категории.
Дата изменения	Дата и время последнего редактирования категории. Данный атрибут отображается только при переходе в режим редактирования.

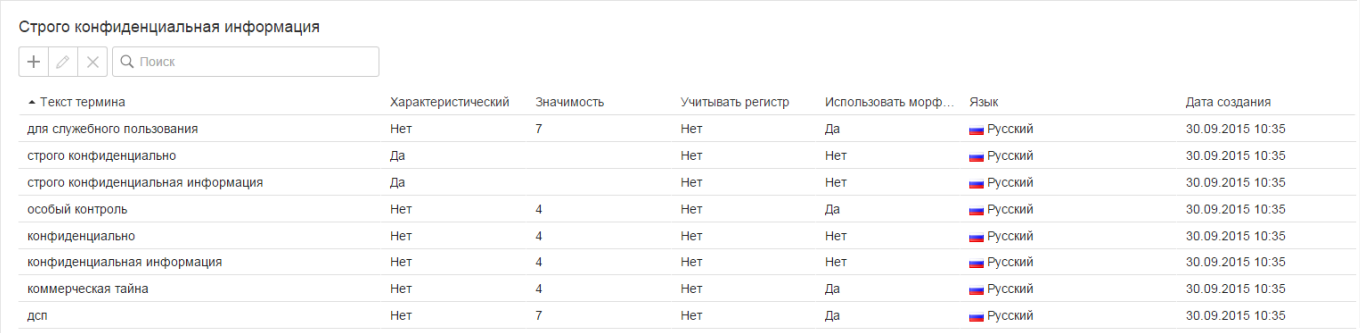
Для того чтобы категория детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Целевые действия пользователя:

- создание предметных областей конфиденциальных данных (см. "Создание категорий и терминов")
- включение категорий в объекты защиты (см. "Создание объекта защиты")

4.4.1.2 Термины

Справочная информация:
Термин - слово или словосочетание, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста той категории, к которой относится найденный термин.


Строго конфиденциальная информация

Поиск

Текст термина	Характеристический	Значимость	Учитывать регистр	Использовать морф…	Язык	Дата создания
для служебного пользования	Нет	7	Нет	Да	Русский	30.09.2015 10:35
строго конфиденциально	Да		Нет	Нет	Русский	30.09.2015 10:35
строго конфиденциальная информация	Да		Нет	Нет	Русский	30.09.2015 10:35
особый контроль	Нет	4	Нет	Да	Русский	30.09.2015 10:35
конфиденциально	Нет	4	Нет	Нет	Русский	30.09.2015 10:35
конфиденциальная информация	Нет	4	Нет	Нет	Русский	30.09.2015 10:35
коммерческая тайна	Нет	4	Нет	Да	Русский	30.09.2015 10:35
дсп	Нет	7	Нет	Да	Русский	30.09.2015 10:35

Атрибуты термина:

Параметр	**Описание**
Текст термина	Слово или словосочетание, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста категории, содержащей термин
Характеристический	Если данный атрибут включен, нахождение в трафике термина обязательно присваивает объекту категорию, содержащую термин
Значимость	Показатель значимости термина
Учитывать регистр	Показатель учета регистра при анализе трафика
Учитывать морфологию	Показатель использования морфологии при анализе трафика
Язык	Язык термина
Дата создания	Дата и время создания термина
Дата изменения	Дата и время последнего изменения термина. Данный атрибут отображается только при переходе в режим редактирования термина.

Примечание:

Настройки параметров **Учитывать регистр** и **Учитывать морфологию для термина** задаются по умолчанию при указании аналогичных параметров для категории. Параметры

термина могут быть отредактированы и сохранены отдельно, но при изменении настроек регистра и морфологии для категории данные изменения не будут повторно применяться к терминологии.

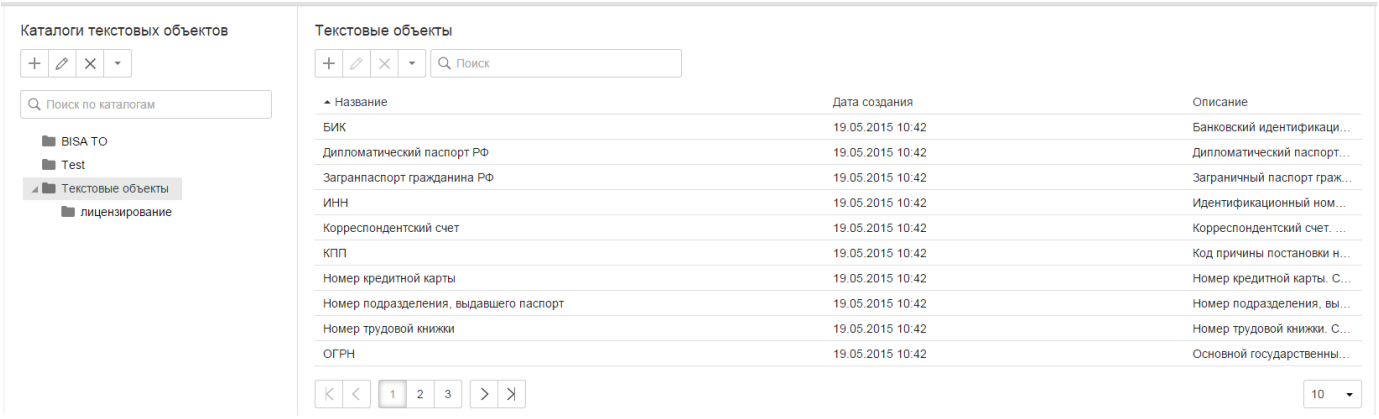
Целевые действия пользователя:

- создание и редактирование терминов (см. "Создание категорий и терминов")

4.4.2 Текстовые объекты

Справочная информация:
Текстовый объект - текстовая информация, извлечённая из тела объекта и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска.

В Системе могут использоваться как системные текстовые объекты, так и текстовые объекты, созданные пользователем.
Т екстовые объекты создаются внутри каталогов. Для работы с каталогами (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. Текстовые объекты, входящие в каталог, и инструменты для работы с текстовыми объектами расположены в правой части рабочей области.



Добавление текстового объекта в каталог выполняется с помощью кнопки + на панели инструментов в правой части рабочей области. Редактирование свойств добавленного текстового объекта выполняется с помощью кнопки , при нажатии на которую открывается окно, где Вы можете просмотреть и при необходимости изменить атрибуты выбранного объекта. Для удаления выбранных текстовых объектов используется кнопка × .

Важно!

При удалении из каталога системного текстового объекта созданные для него пользовательские шаблоны будут удалены из Системы .

Атрибуты текстового объекта:

Параметр	Описание
Название	Наименование категории
Дата создания	Дата и время создания текстового объекта
Дата изменения	Дата и время изменения текстового объекта. Данный атрибут отображается только при переходе в режим редактирования текстового объекта
Шаблоны текстовых объектов	Значения текстового объекта, заданные в виде точной последовательности символов либо с помощью регулярного выражения. Данный атрибут отображается только при переходе в режим редактирования текстового объекта
Описание	Примечание в произвольной форме

Для того чтобы текстовый объект детектировался в перехваченных данных, его необходимо включить в объект защиты.

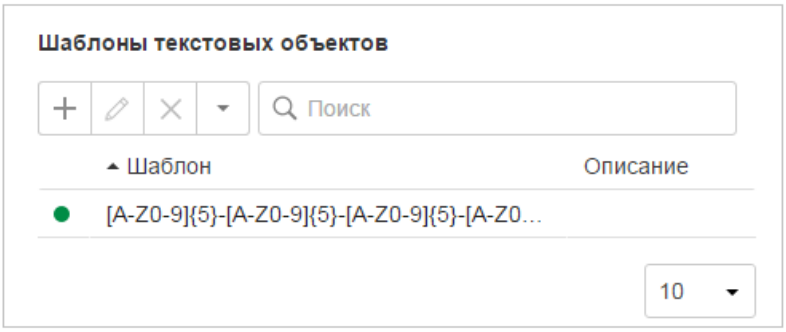
Целевые действия пользователя:

- создание текстовых объектов и их каталогов (см. "Работа с текстовыми объектами");
- добавление системных текстовых объектов в выбранный каталог (см. "Работа с текстовыми объектами");
- импорт и экспорт текстовых объектов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- добавление текстовых объектов в объекты защиты (см. "Создание объекта защиты")

4.4.2.1 Шаблоны текстовых объектов

Справочная информация:
Шаблон текстового объекта - значение текстового объекта, заданное в виде точной последовательности символов либо с помощью регулярного выражения. С помощью шаблона для каждого текстового объекта может быть задано одно или несколько значений.

Шаблоны для выбранного текстового объекта отображаются при переходе в режим редактирования текстового объекта.

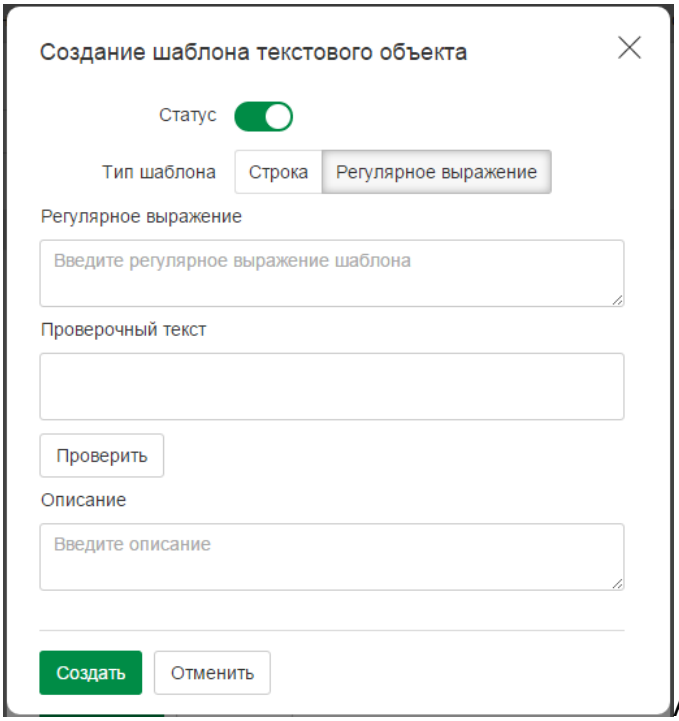


Используя кнопки на панели инструментов, Вы можете добавить новый шаблон (кнопка), перейти в режим редактирования выбранного шаблона (кнопка), удалить выбранные шаблоны (кнопка), а также изменить статус шаблона (нажмите кнопку и в раскрывающемся списке выберите **Активировать/Деактивировать**). Текущий статус шаблона отображается в левом столбце таблицы: активные шаблоны отмечены пиктограммой , неактивные - пиктограммой .

Важно!

Изменение и удаление предустановленных шаблонов для системных текстовых объектов недоступно.

При добавлении шаблона открывается окно создания шаблона, в котором нужно указать атрибуты шаблона.



Атрибуты шаблона:

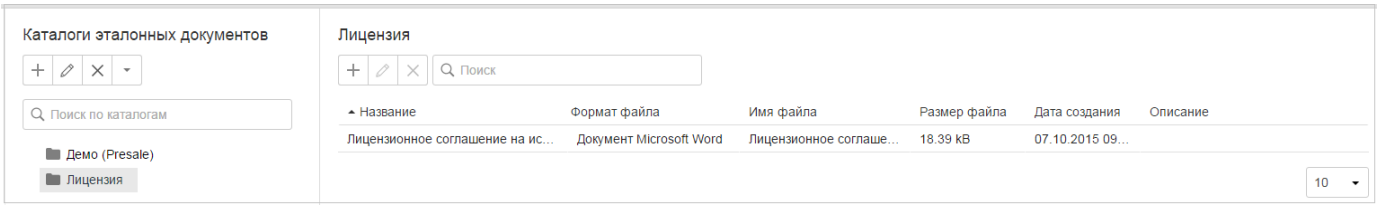
Параметр	Описание
Статус	Показатель того, используется ли данный шаблон. Может принимать значения: *Активный* и *Неактивный.*
Тип шаблона	Укажите, каким образом будет задан шаблон: в виде строки или регулярного выражения.
Строка	Отображается, если выбран тип шаблона - *Строка*. Точное значение текстового объекта, заданное в виде последовательности символов. *Например*, шаблон `example@company.com` выявит в тексте только точное совпадение - `example@company.com`
Регулярное выражение	Отображается, если выбран тип шаблона - *Регулярное выражение*. Настраиваемый шаблон. Подробнее о создании настраиваемого шаблона см. в интернет-статье "Элементы языка регулярных выражений".
Проверочный текст	Отображается, если выбран тип шаблона - *Регулярное выражение*. Пример текста для проверки нахождения регулярного выражения. Введите проверочный текст в поле и нажмите **Проверить**.
Описание	Примечание в произвольной форме

Целевые действия пользователя:

- Создание текстового объекта

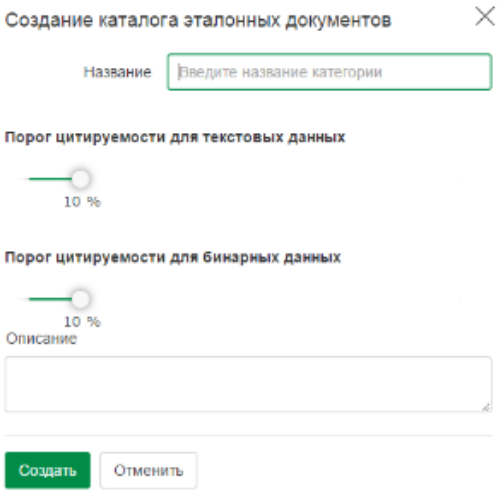
4.4.3 Эталонные документы

Справочная информация:
Эталонный документ - документ, цитаты из которого ищутся в анализируемом тексте. Эталонными документами могут быть образцы текстов приказов, финансовых отчетов, договоров и других конфиденциальных документов. Эталонные документы хранятся в Системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы. Эталонные документы в Системе сгруппированы в каталоги.



Список эталонных документов

При нажатии на кнопку  на панели инструментов в левой части рабочей области открывается окно создания нового каталога, где Вы можете указать его атрибуты.

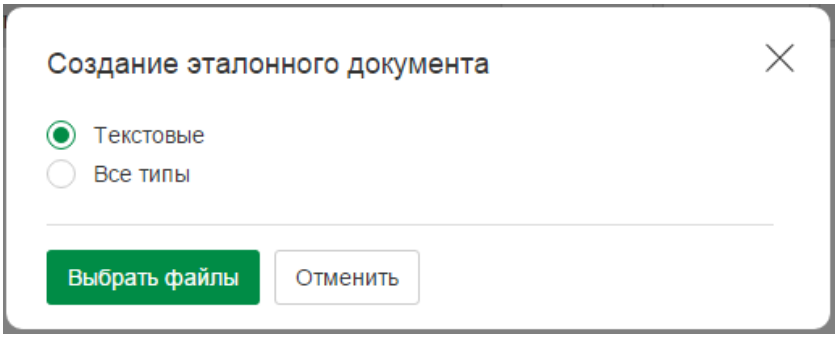


Атрибуты каталога эталонных документов:

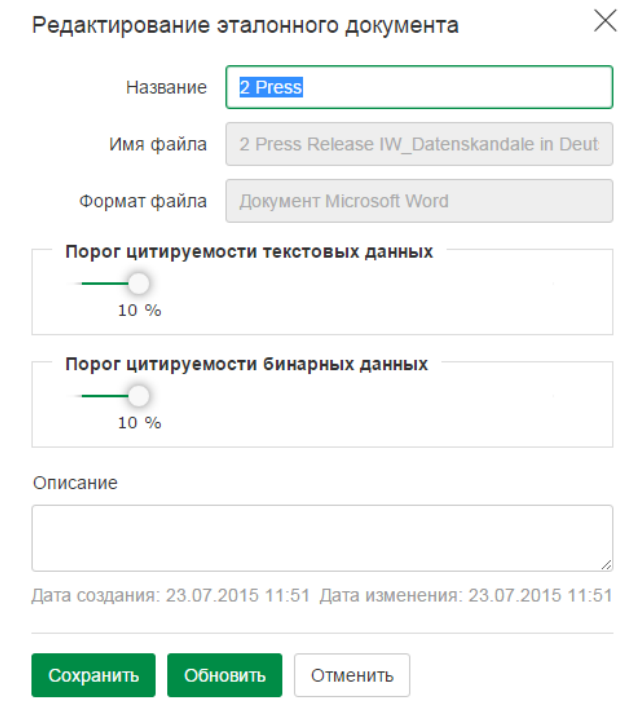
Параметр	Описание
Название	Название каталога эталонных документов
Порог цитируемости для текстовых данных	Процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Для детектирования текстовых объектов (текста документов).
Порог цитируемости для бинарных данных	Процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Для детектирования бинарных объектов (рисунков, исполнимых файлов и проч.).

Параметр	Описание
Описание	Описание в произвольной форме

Добавление файла эталонного документа в созданный каталог выполняется с помощью кнопки на панели инструментов в правой части рабочей области. В открывшемся диалоговом окне вы можете указать тип добавляемых данных (**Текстовые** или **Все типы**) и выбрать файлы для загрузки.



Редактирование свойств добавленного эталонного документа выполняется с помощью кнопки на панели инструментов. В открывшемся окне Вы можете просмотреть и при необходимости изменить атрибуты выбранного эталонного документа.



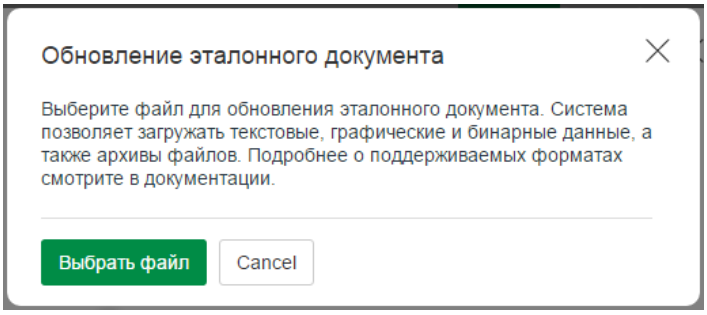
Окно редактирования эталонного документа

Атрибуты эталонного документа:

Параметр	Описание
Название	Название эталонного документа

Параметр	Описание
Имя файла	Имя файла, загруженного в качестве эталонного документа
Формат файла	Формат файла: текст, изображение и др.
Размер файла	Размер файла, загруженного в качестве эталонного документа
Дата создания	Дата и время создания эталонного документа
Дата изменения	Дата и время последнего изменения эталонного документа. Данный атрибут отображается только при переходе в режим редактирования.
Порог цитируемости для текстовых данных	Процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Для детектирования текстовых объектов (текста документов). Данный атрибут отображается только при переходе в режим редактирования.
Порог цитируемости для бинарных данных	Процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Для детектирования бинарных объектов (рисунков, исполняемых файлов и проч.). Данный атрибут отображается только при переходе в режим редактирования.
Описание	Описание в произвольной форме

Переход в режим обновления эталонного документа выполняется с помощью кнопки **Обновить** в окне редактирования документа.



Для того чтобы эталонный документ детектировался в перехваченных данных, его необходимо включить в объект защиты.

Целевые действия пользователя:

- Создание эталонных документов и их каталогов (см. "Работа с эталонными документами")
- Импорт и экспорт эталонных документов в составе базы технологий ("Экспорт и импорт базы технологий")
- Обновление эталонного документа ("Работа с эталонными документами")
- Добавление эталонных документов в объекты защиты ("Создание объекта защиты")

4.4.4 Бланки

Справочная информация:
Эталонный бланк - бланк, версия которого ищется в сетевом трафике. Эталонные бланки хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни

пользователям, ни администраторам Системы.
В качестве эталонных бланков могут выступать анкеты, опросные листы и другие документы, заполняемые по заранее заданной форме.
На техническом уровне эталонный бланк – это файл, каждая строка которого содержит одно поле бланка, строки отделяются друг от друга переносом строки, и бланк содержит минимум 2 поля.

Для того чтобы эталонный бланк детектировался в перехваченных данных, его необходимо включить в объект защиты.

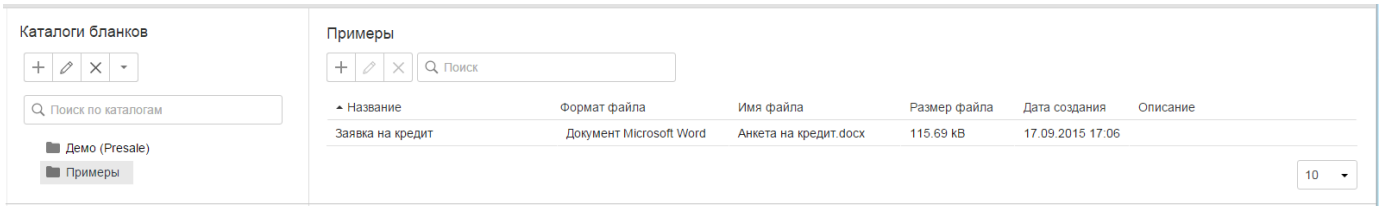
Важно!

Для соотнесения объекта перехвата с объектом защиты, содержащим эталонный бланк, необходимо, чтобы выполнялись следующие условия:

- в тексте объекта должно содержаться хотя бы одно поле из эталонного бланка;
- если количество обнаруженных в тексте объекта полей более одного, то поля должны располагаться в том порядке, который имеется в загруженном в Систему цифровом отпечатке;
- если установлено детектирование только заполненных бланков, то между парой соседних строк должен быть хотя бы один символ.

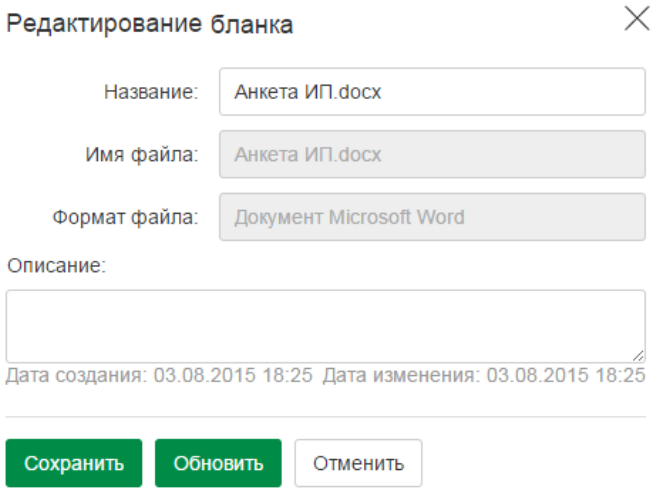
Принцип работы технологии: осуществляется поиск наименования полей бланка в тексте события и затем проверяется порядок их следования, при необходимости проверяется присутствие текста между полями бланка, на базе чего определяется, был ли бланк заполнен.

Эталонные бланки создаются внутри каталогов. Для работы с каталогами бланков (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. Эталонные бланки, входящие в каталог, и инструменты для работы с бланками расположены в правой части рабочей области.



Список эталонных бланков и их каталогов

Добавление файла эталонного бланка в каталог выполняется с помощью кнопки  на панели инструментов в правой части рабочей области. Редактирование свойств добавленного эталонного бланка выполняется с помощью кнопки , при нажатии на которую открывается окно, где Вы можете просмотреть и при необходимости изменить атрибуты выбранного бланка.

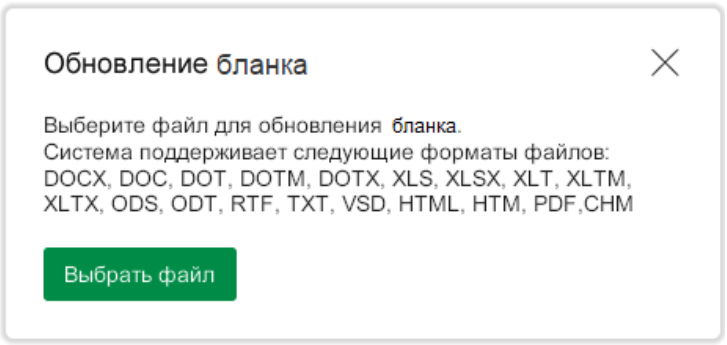


Окно редактирования эталонного бланка

Атрибуты эталонного бланка:

Параметр	**Описание**
Название	Наименование эталонного бланка
Тип файла	Формат файла. Поддерживаются следующие форматы: DOCX, DOC, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF,CHM
Имя файла	Формат файла, загруженного в качестве эталонного бланка
Описание	Примечание в произвольной форме
Дата создания	Дата и время создания бланка
Дата изменения	Дата и время последнего изменения бланка. Данный атрибут отображается только при переходе в режим редактирования бланка.

Переход в режим обновления эталонного бланка выполняется с помощью кнопки **Обновить** в окне редактирования бланка.



Целевые действия пользователя:

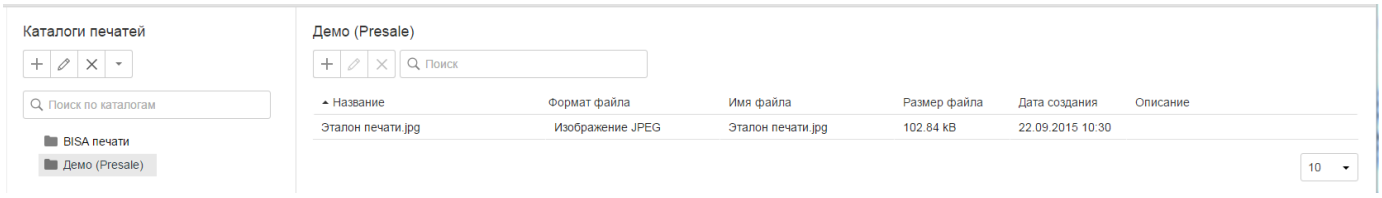
- создание эталонных бланков и их каталогов (см. "Работа с бланками")
- импорт и экспорт бланков в составе базы технологий ("Экспорт и импорт базы технологий")
- обновление эталонного бланка ("Работа с бланками")

- добавление эталонных бланков в объекты защиты ("Создание объекта защиты")

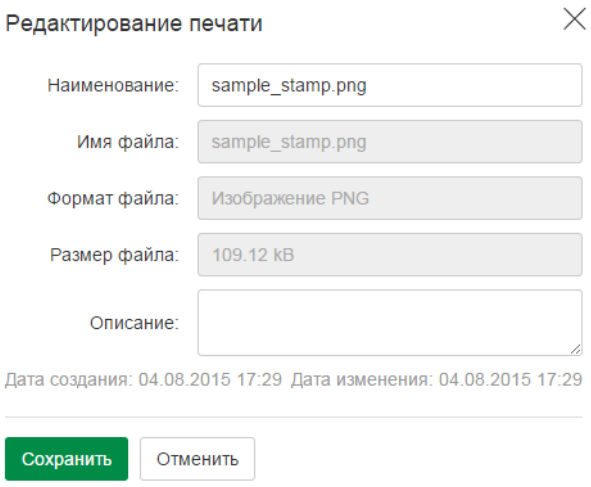
4.4.5 Печати

Справочная информация:
Эталонная печать - изображение печати, которое ищется в сетевом трафике. Эталонными печатями могут быть изображения круглых оттисков, которые используются в организациях.

Эталонные печати создаются внутри каталогов. Для работы с каталогами печатей (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. Эталонные печати, входящие в каталог, и инструменты для работы с печатями расположены в правой части рабочей области.



Добавление файла эталонной печати в каталог выполняется с помощью кнопки  на панели инструментов в правой части рабочей области. Редактирование свойств добавленной эталонной печати выполняется с помощью кнопки , при нажатии на которую открывается окно, где Вы можете просмотреть и при необходимости изменить атрибуты выбранной печати.



Окно редактирования эталонной печати

Атрибуты эталонной печати:

Параметр	Описание
Наименование	Наименование эталонной печати
Формат файла	Формат изображения. Поддерживаются следующие форматы: BMP, DIB, JPEG, JPG, JPE, JP2, PNG, PBM, PGM, PPM, SR, RAS, TIF, TIFF.
Имя файла	Название файла, загруженного в качестве эталонной печати
Размер файла	Размер файла, загруженного в качестве эталонной печати
Описание	Примечание в произвольной форме

Параметр	Описание
Дата создания	Дата и время создания эталонной печати
Дата изменения	Дата и время последнего изменения эталонной печати. Данный атрибут отображается только при переходе в режим редактирования.

Для того чтобы эталонная печать детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Целевые действия пользователя:

- создание эталонный печатей и их каталогов (см. "Работа с эталонными печатями")
- добавление эталонных печатей в объекты защиты (см. "Создание объекта защиты")
- экспорт и импорт эталонных печатей в составе базы технологий (см. "Экспорт и импорт базы технологий")

4.4.6 Выгрузки из БД

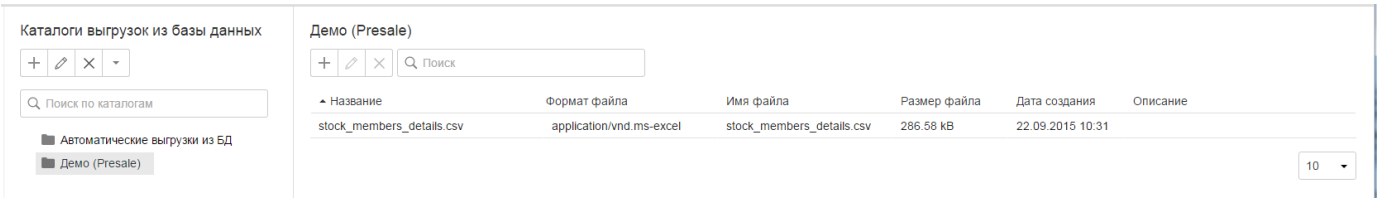
Справочная информация:
Эталонная выгрузка из БД - часть базы данных, цитаты из которой ищутся в анализируемом тексте. Эталонными выгрузками из БД могут быть списки заработных плат сотрудников, личные данные и прочее.

Важно!

Для корректной работы в Системе эталонная выгрузка из БД должна иметь следующие характеристики:

- количество столбцов - не более 32;
- количество слов в ячейке - не более 256;
- количество строк - не более 1 млн (при объеме оперативной памяти сервера 8 ГБ) или не более 3,5 млн (при объеме оперативной памяти сервера 16 ГБ);
- размер выгрузки - не более 1Гб, если используется База данных Postgre SQL.

Эталонные выгрузки создаются внутри каталогов. Для работы с каталогами выгрузок (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. Эталонные выгрузки, входящие в каталог, и инструменты для работы с выгрузками расположены в правой части рабочей области.



Предустановленный каталог **Автоматические выгрузки из БД** содержит эталонные выгрузки, полученные от внешней системы (подробнее см. "Автоматически обновляемые выгрузки из БД").

Примечание.

Каталог **Автоматические выгрузки из БД** является системным, и для него недоступна операция удаления.

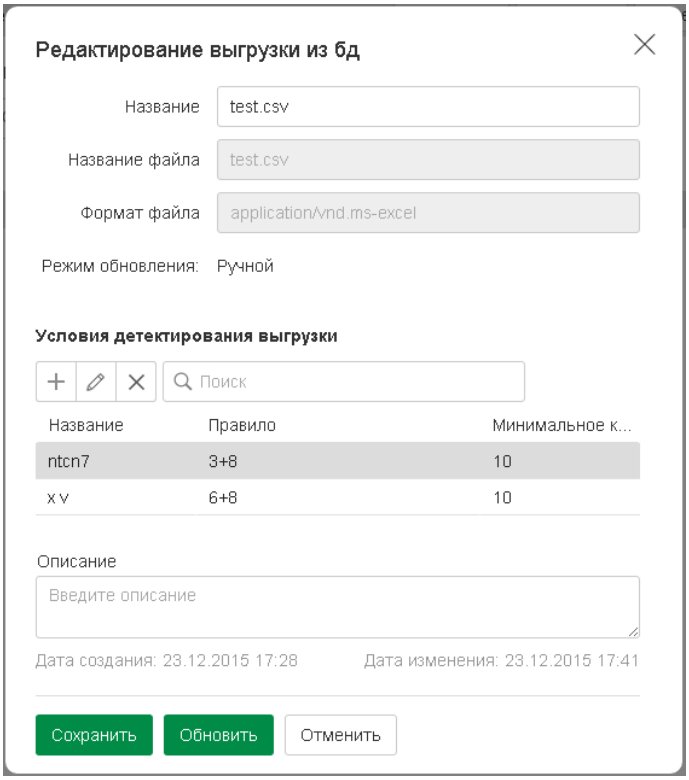
Добавление файла эталонной выгрузки в каталог выполняется с помощью кнопки на панели инструментов в правой части рабочей области.

При загрузке файла эталонной выгрузки выполняется его компиляция. Объем оперативной памяти, потребляемой при компиляции, можно приблизительно определить по следующей формуле:

`Память(GB) = 0.05 * уникальных_слов (M) * ячеек (M)`, где M - миллион.

Например, 10 миллионов ячеек могут поместиться в таблицу с 2 столбцами и 5 миллионами строк, либо в таблицу с 4 столбцами и 2,5 миллионами строк.

Редактирование свойств добавленной эталонной выгрузки выполняется с помощью кнопки на панели инструментов в правой части рабочей области. В открывшемся окне Вы можете просмотреть и при необходимости изменить атрибуты выбранной выгрузки.



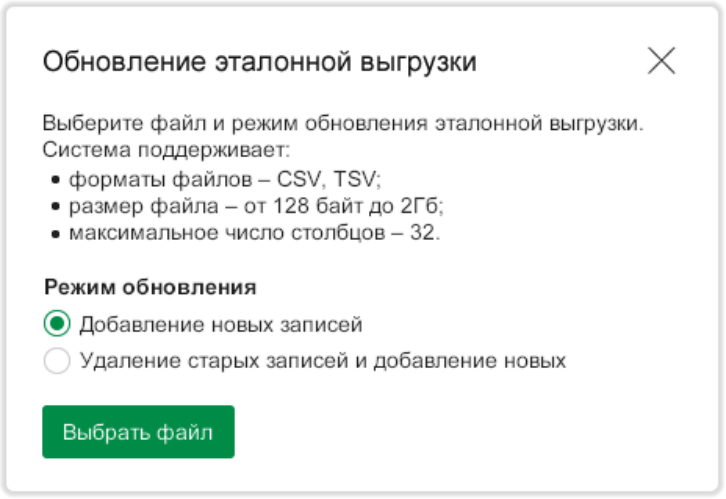
Атрибуты эталонной выгрузки из БД:

Параметр	Описание

Параметр	Описание
Название	Наименование эталонной выгрузки
Имя файла	Название файла, загруженного в качестве эталонной выгрузки из БД
Формат файла	Разновидность файла
Режим обновления	Возможные варианты: **Ручной** или **Автоматический**
Описание	Примечание в произвольной форме
Дата создания	Дата и время создания выгрузки
Дата изменения	Дата и время последнего изменения выгрузки. Данный атрибут отображается только при переходе в режим редактирования выгрузки
Условия детектирования выгрузки	Описание логических взаимоотношений между столбцами таблицы и минимальное количество непустых строк в таблице, требуемое для срабатывания эталонной выгрузки.

В области **Условия детектирования выгрузки** отображается панель инструментов для работы с условиями и список добавленных условий.

Переход в режим обновления эталонной выгрузки выполняется с помощью кнопки **Обновить** в окне редактирования выгрузки.



Для того чтобы эталонная выгрузка детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Целевые действия пользователя:

- создание эталонных выгрузок из БД и их каталогов (см. "Работа с эталонными выгрузками")
- обновление эталонной выгрузки (см. "Работа с эталонными выгрузками")
- добавление условий детектирования выгрузки (см. "Условия детектирования выгрузки")
- автоматическое обновление эталонной выгрузки (см. "Автоматически обновляемые выгрузки из БД")
- добавление эталонных выгрузок в объекты защиты ("Создание объекта защиты")

4.4.6.1 Автоматически обновляемые выгрузки из БД

Автоматически обновляемые выгрузки из БД - это выгрузки, созданные внешней системы. Внешняя система (коннектор) инициирует добавление и последующее обновление автоматических выгрузок.

Важно!

Одновременное редактирование конфигурации через Консоль управления и через SDK может вызвать конфликт, поэтому при разработке коннектора рекомендуется ознакомиться с общими принципами работы с конфигурацией Системы. В случае возникновения конфликта следует, в первую очередь, просмотреть ошибки, возвращаемые коннектору от SDK.

Эталонные выгрузки, созданные внешней системой, помещаются в предустановленный каталог **Автоматические выгрузки из БД**. Авторизация внешней системы в Traffic Monitor осуществляется с помощью плагина (об установке плагина см. документ "*InfoWatch Traffic Monitor. Руководство администратора*").

Примечание.

Просмотр и редактирование каталога **Автоматические выгрузки из БД** доступны при наличии лицензии на использование данной технологии.

Атрибуты автоматической выгрузки формируются на основе данных, переданных от внешней системы:

Параметр	Описание
Наименование	Название файла выгрузки в Системе
Источник обновления	Система - источник файла выгрузки
Комментарий к выгрузке	Сопроводительная информация
Условие срабатывания	Детектирование всех заполненных столбцов. Минимальное количество столбцов - 10 *Например:* При количестве столбцов 3, условие будет иметь следующий вид: 1+2+3, минимальное количество строк - 10.

Вы также можете добавить эталонные выгрузки в каталог **Автоматические выгрузки из БД** вручную с помощью кнопки



на панели инструментов в правой части рабочей области. Для эталонных выгрузок, добавленных вручную, обновление будет выполняться стандартным способом (см. "Работа с выгрузками").

Примечание.

При создании новой выгрузки файл выгрузки может быть пустым, если:

- загрузка содержимого завершилась принудительно;
- при загрузке содержимого оборвалась связь;
- валидация содержимого завершилась с ошибкой.

Если в Системе создалась пустая выгрузка, то при восстановлении работоспособности стороннее приложение может воспользоваться уже созданной пустой выгрузкой и наполнить ее, не создавая выгрузку заново.

Для всех эталонных выгрузок, содержащихся в каталоге доступны операции редактирования и удаления. Данные операции выполняются с помощью кнопок на панели инструментов в правой части рабочей области.

Внимание!

При удалении эталонной выгрузки, созданной внешней системой, автоматическое обновление данной выгрузки будет недоступно.

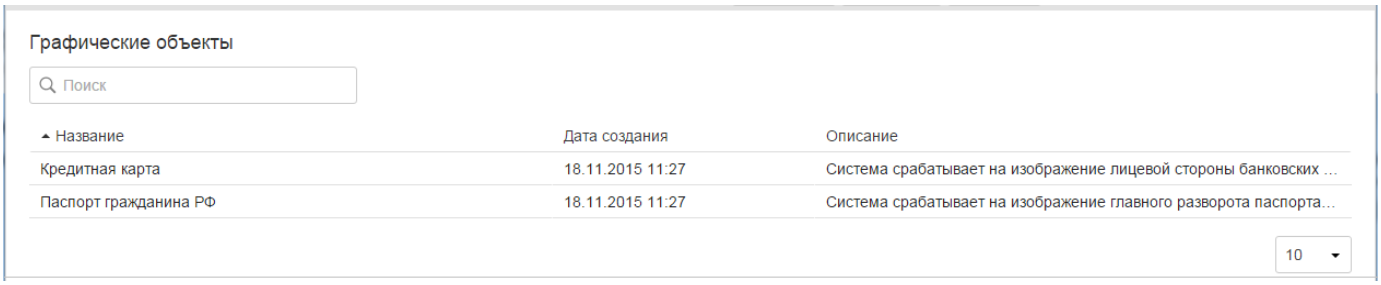
Для того чтобы автоматическая эталонная выгрузка детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

4.4.7 Графические объекты

Справочная информация:

Графический объект - изображение, извлечённое из тела объекта и его вложений. Наличие в изображении определенных признаков позволяет отнести его к какому-либо классу предустановленных графических объектов.

Графические объекты используются при создании объектов защиты.



Атрибуты графического объекта:

Параметр	Описание
Название	Название графического объекта
Дата создания	Дата и время создания объекта

Параметр	Описание
Описание	Описание графического объекта

В Системе могут содержаться следующие графические объекты (набор графических объектов определяется типом лицензии):

Название	Описание
Паспорт гражданина РФ	Изображение главного разворота паспорта гражданина РФ (стр. 2-3)
Кредитная карта	Изображение лицевой стороны банковских карт VISA, Visa Electron, MasterCard, Maestro
Географические карты	Географическая карта или ее часть
Технические чертежи	Чертежи, представляющие собой набор черных линий на белом фоне

В Системе используются только предустановленные графические объекты с заранее заданными атрибутами. Добавление, редактирование и удаление графических объектов недоступно.

Для того чтобы графический объект детектировался в перехваченных данных, его необходимо включить в объект защиты.

Целевые действия пользователя:

- создание объекта защиты с использованием графических объектов (см. "Создание объекта защиты").

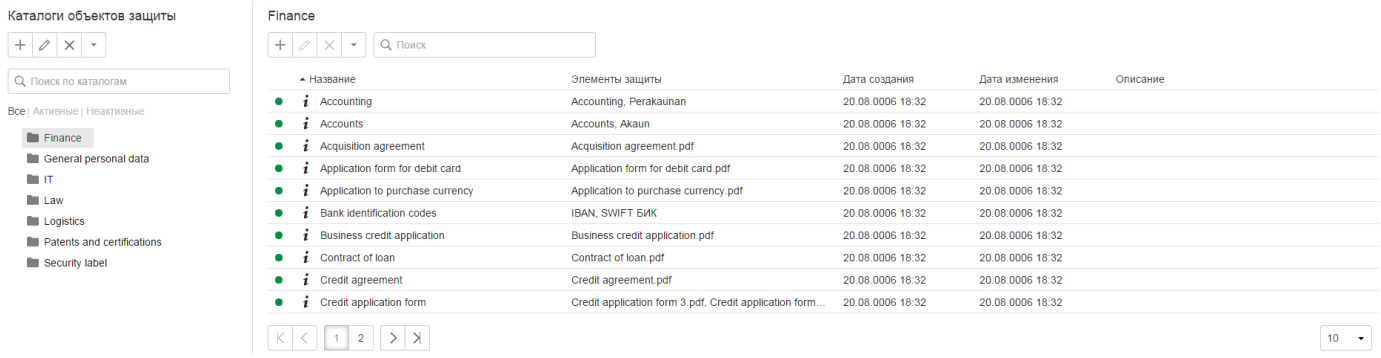
4.5 Раздел "Объекты защиты"

Справочная информация:

Объект защиты представляет собой совокупность элементов анализа содержимого событий. Объекты защиты используются для определения соответствия перехваченных данных определенным бизнес-документам.

О разделе:

Раздел содержит объекты защиты, сгруппированные в каталоги, и инструменты для работы с ними.



Список каталогов содержит как пользовательские, так и предустановленные каталоги объектов защиты.

Каждый каталог имеет статус (*Активный* или *Неактивный*). Статус каталога применяется ко всем вложенным каталогам и входящим в них объектам защиты.

В правой части рабочей области отображаются объекты защиты для выбранного каталога. Для каждого объекта защиты отображается его статус (*Активный*



или *Неактивный*



), название, входящие в объект защиты элементы анализа, даты создания и последнего изменения объекта защиты, описание.

При создании нового объекта защиты отображается окно добавления элементов анализа, где вы можете выбрать элементы, на основе которых будет создан объект защиты (подробнее о технологиях, используемых в Системе, см. "Определение конфиденциальной информации").

Примечание.

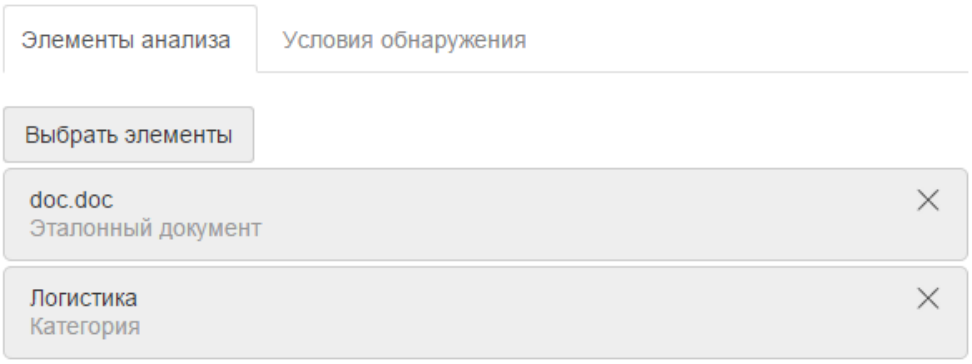
Если выбрана настройка **Создать объект защиты на каждый выбранный элемент**, то для каждого элемента анализа будет создан отдельный объект защиты. Атрибуты объектов защиты задаются Системой по умолчанию.

Целевые действия пользователя:

- Создание каталога объектов защиты
- Создание объекта защиты
- Добавление элементов анализа
- Создание политики для объектов защиты и их каталогов
- Импорт и экспорт объектов защиты

4.5.1 Элементы анализа

Справочная информация:
Элементы анализа - элементы настройки технологий, на основе которых формируются объекты защиты (например, текстовые объекты, эталонные документы и прочее).



Раздел **Объекты защиты**, вкладка **Элементы анализа** при создании или редактировании объекта защиты

Вкладка **Элементы анализа** отображается при создании объекта защиты, после того как требуемые элемента выбраны в окне добавления элементов анализа, или при переходе в режим редактирования ранее созданного объекта защиты.

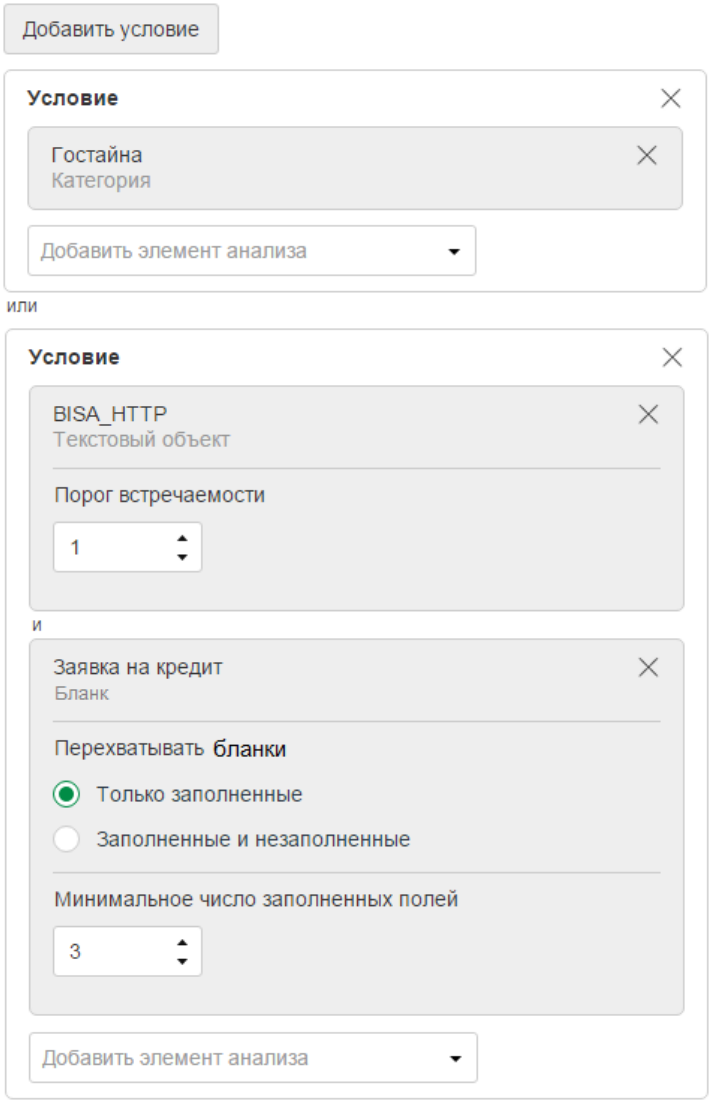
На вкладке **Элементы анализа** вы можете добавить дополнительные элементы в объект защиты (кнопка **Выбрать элементы**) или удалить элемент анализа (кнопка X в правом верхнем углу панели элемента).

Условия детектирования добавленных элементов анализа указываются на вкладке **Условия обнаружения**.

Целевые действия пользователя:

- Добавление элементов анализа

4.5.2 Условия обнаружения



Вкладка **Условия обнаружения**, отображаемая при создании или редактировании объекта защиты

Вы можете указать условия детектирования при создании объекта защиты, после того как требуемые элемента выбраны в окне добавления элементов анализа, или при переходе в режим редактирования ранее созданного объекта защиты.

Условия обнаружения могут быть добавлены внутри одного блока и объединены с помощью операции конъюнкции (логическое "И"), либо добавлены в различные блоки, объединенные между собой с помощью операции дизъюнкции (логическое "ИЛИ").

Условия обнаружения элементов анализа:

Название элемента	Условие обнаружения
Эталонный документ	Проверяется, содержит ли объект перехвата указанный эталонный документ
Категория	Проверяется соответствие объекта перехвата указанной категории. Для категорий, содержащих подкатегории, проверяется соответствие объекта перехвата какой-либо подкатегории.

Название элемента	Условие обнаружения
Текстовый объект	Проверяется, содержит ли объект перехвата указанный текстовый объект. Дополнительное условия обнаружения - порог встречаемости. Опредяляет, сколько раз минимум тестовый объект должен присутствовать в объекте перехвата. Значение по умолчанию - 3. В зависимости от типа используемого шаблона количество вхождений текстового объекта определяется следующим образом: • если шаблон текстового объекта задан в виде регулярного выражения, то одно его значение, найденное в пределах одного документа несколько раз, считается одним вхождением; • если шаблон текстового объекта задан в виде строки, то считаются все его вхождения.
Бланк	Проверяется, содержит ли объект перехвата хотя бы один из указанных эталонных бланков. Дополнительные условия обнаружения: • поиск по заполненным и незаполненным бланкам. Если требуется, чтобы детектировались все бланки, установите флажок в поле **Заполненные и незаполненные**. По умолчанию выполняется детектирование заполненных бланков; • минимальное число совпадающих записей. Значение по умолчанию - 3.
Печать	Проверяется, содержит ли объект перехвата указанную эталонную печать
Графический объект	Проверяется, содержит ли объект перехвата указанный графический объект
Выгрузка из базы данных	Проверяется, содержит ли объект перехвата указанную эталонную выгрузку. Необходимо выбрать одно из представлений выгрузки

См. также: Элементы анализа

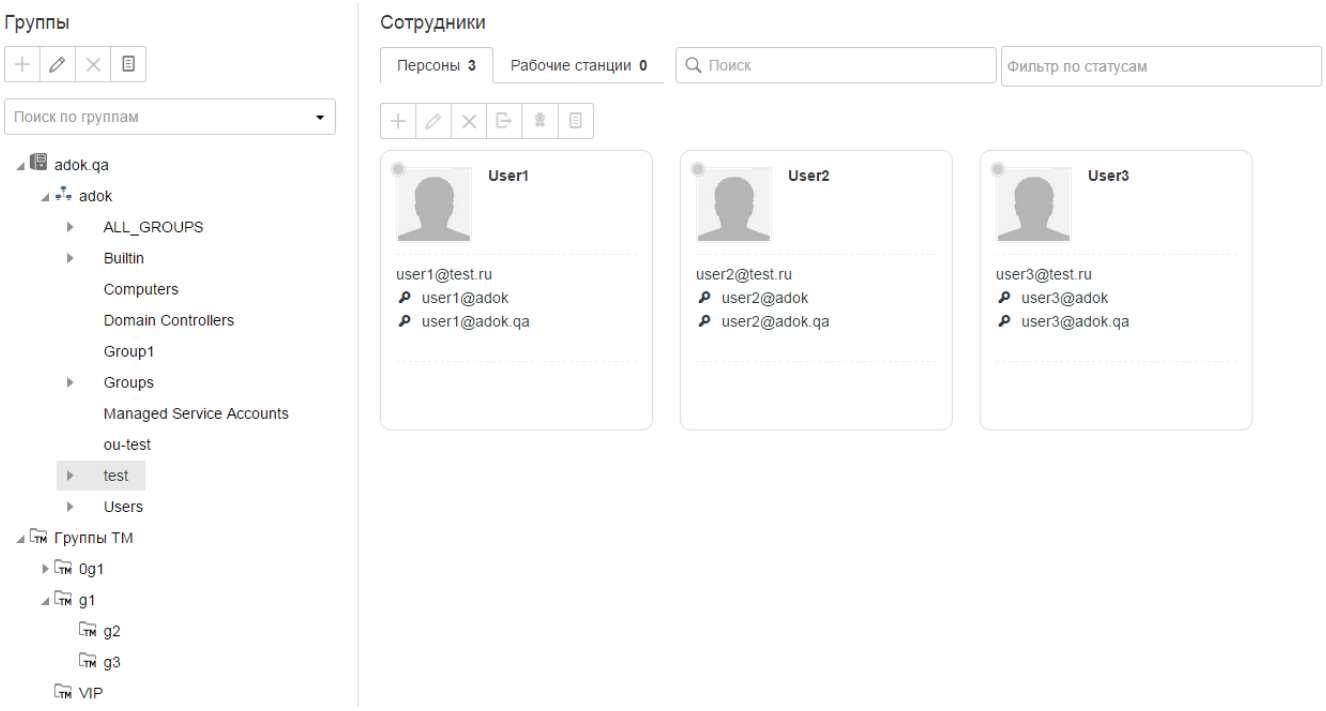
Целевые действия пользователя:

- Добавление условий обнаружения

4.6 Раздел "Персоны"

Справочная информация:
Наличие списков персон и рабочих станций облегчает офицеру безопасности работу с перехваченными объектами. Это происходит за счет учета информации об отправителях и получателях (персонах), а также рабочих станциях с помощью специальных справочников.

О разделе:
Раздел содержит справочник персон и рабочих станций информационной системы организации.



Раздел **Персоны**

Важно!

При превышении допустимого в текущей лицензии количества персон, события от которых обрабатываются, в верхней части окна браузера отображается сообщение вида: **Внимание! Лицензионный порог кол-ва сотрудников, события от которых обрабатывает Система, превышен на 1.**

Данное сообщение имеет информационный характер и не влияет на работоспособность Системы.
Количество персон, события от которых обрабатываются в Системе, соответствует количеству персон, которые за последние 30 дней отправляли какой-либо тип трафика.
Допустимое в текущей лицензии количество персон отображается в сведениях о лицензии, в атрибуте **Лицензировано пользователей** (подробнее см. документ «*Infowatch Traffic Monitor. Руководство администратора*»).

В разделе содержатся следующие элементы:

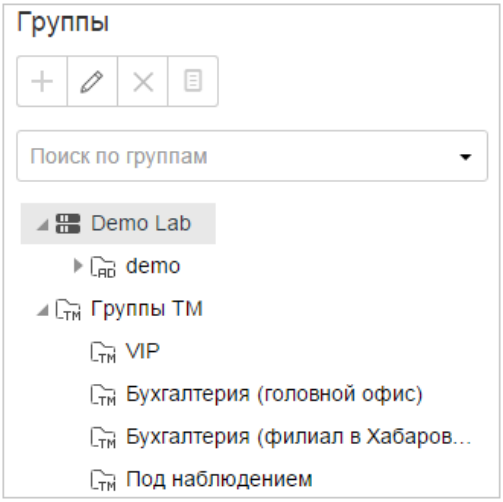
Элемент	Назначение
Группы персон/рабочих станций из Active Directory	Расположен в левой части рабочей области. Содержит структуру организации, полученную из Active Directory.
Группы персон/рабочих станций из Domino Directory	Расположен в левой части рабочей области. Содержит структуру организации, полученную из Domino Directory.
Группы персон/рабочих станций, созданные средствами Traffic Monitor	Расположен в левой части рабочей области. Содержит структуру организации, созданную средствами Traffic Monitor.

Элемент	Назначение
Вкладка **Персоны** для выбранной группы	Расположен в правой части рабочей области. Содержит список персон, входящих в выделенную группу.
Вкладка **Рабочие станции** для выбранной группы	Расположен в правой части рабочей области. Содержит список рабочих станций, входящих в выделенную группу.
Панели инструментов	Набор инструментов для групп, персон и рабочих станций
Поле **Поиск по группам**	Фильтрация групп персон и рабочих станций
Поле **Поиск**	Фильтрация персон и рабочих станций
Поле **Фильтр по статусам**	Фильтрация персон и рабочих станций по атрибуту **Статус**

Целевые действия пользователя:

- Создание группы персон и рабочих станций (см. "Создание группы персон и рабочих станций")
- Создание списка персон и рабочих станций (см. "Создание персон и рабочих станций")
- Просмотр виджетов с информацией о персонах и рабочих станциях (см. "Просмотр сводки по персоне/рабочей станции")
- Создание фильтра по персонам и рабочим станциям (см. "Просмотр событий по персоне/рабочей станции")
- Формирование политики для персон и рабочих станций (см. "Добавление персоны/рабочей станции в политику")
- Работа со статусами персон и рабочих станций (см. "Добавление статуса персоне/рабочей станции")
- Добавление персон и рабочих станций в периметры (см. "Добавление персоны/рабочей станции в периметр компании")

4.6.1 Группы персон и рабочих станций



Примечание:

Группы, для которых была выполнена синхронизация с Active Directory, отмечены значком .

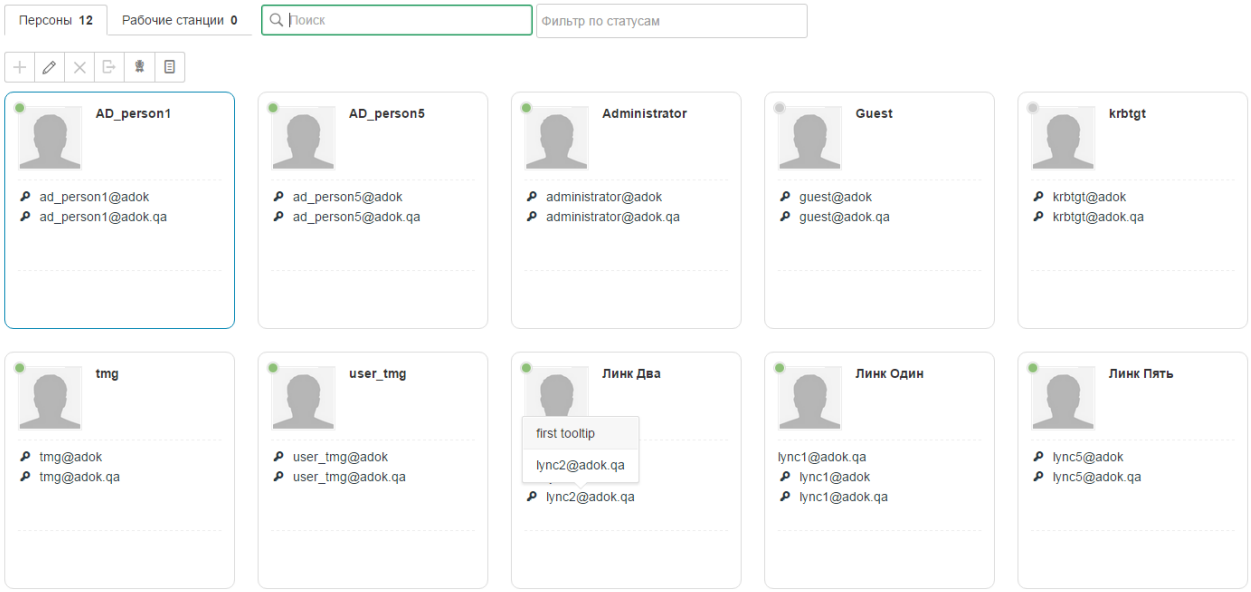
Атрибуты группы персон и рабочих станций:

Параметр	Описание
Имя	Наименование группы
Контакты	Контактные данные группы
Содержит группы	Список групп, входящих в данную группу
Входит в группы	Список групп, в которые входит данная группа
Примечание	Описание в произвольной форме

Целевые действия пользователя:

- Создание группы персон и рабочих станций

4.6.2 Персоны



Примечание:

Для персон, данные которых импортированы из Active Directory, отображается цветовой индикатор в левом верхнем углу фотографии профиля:

- для активных сотрудников;

- для сотрудников, отключенных в AD.

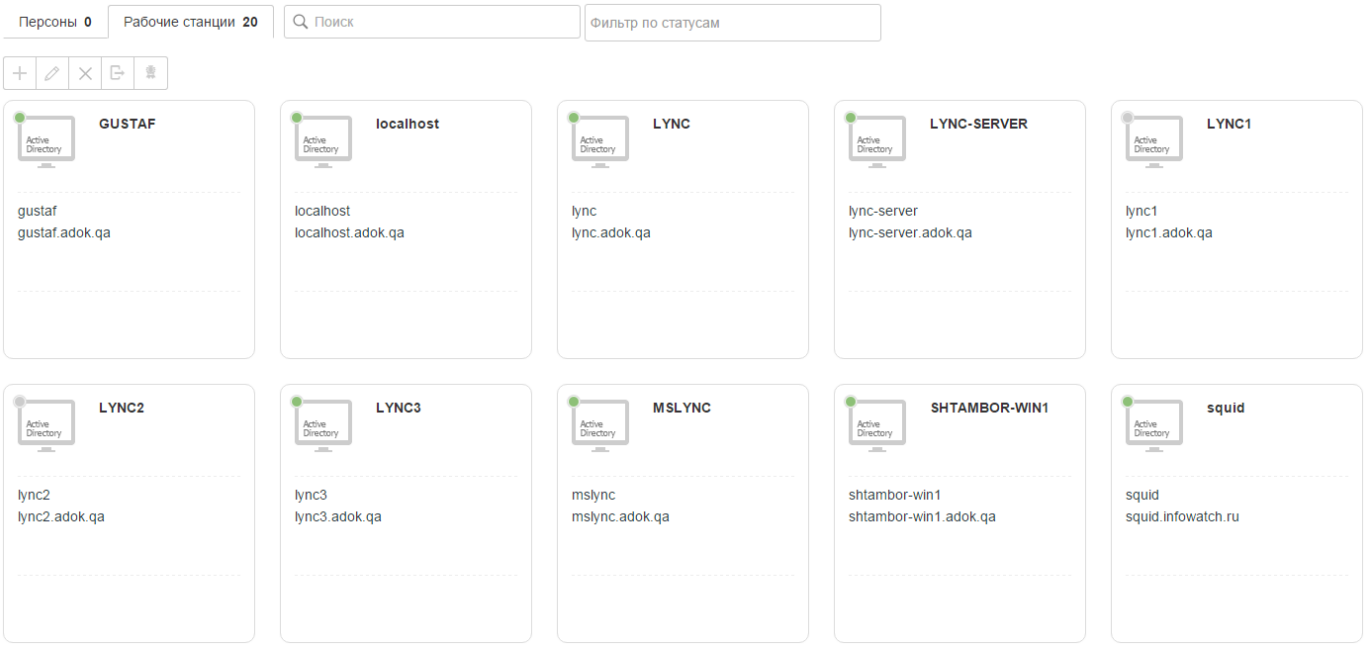
Атрибуты персоны:

Параметр	Описание
Фамилия	Фамилия персоны
Имя	Имя персоны
Сотрудник/Не сотрудник	Индикатор того, является ли персона сотрудником компании
Должность	Должность персоны
Отдел	Отдел, в котором работает персона
Комната	Комната, в которой работает персона
Руководитель	Руководитель персоны
Примечание	Произвольное описание
Контакты	Контакты персоны (офицер безопасности может указать домашние или рабочие контакты, включая адрес электронной почты, номер телефона, логин Skype, ICQ или адрес сайта в Интернет)
Группы	Группы, в которые включена персона
Рабочие станции	Рабочие станции, привязанные к учетной записи персоны
Статусы	Статус, который присваивает персоне офицер безопасности
Фото	Фотография персоны

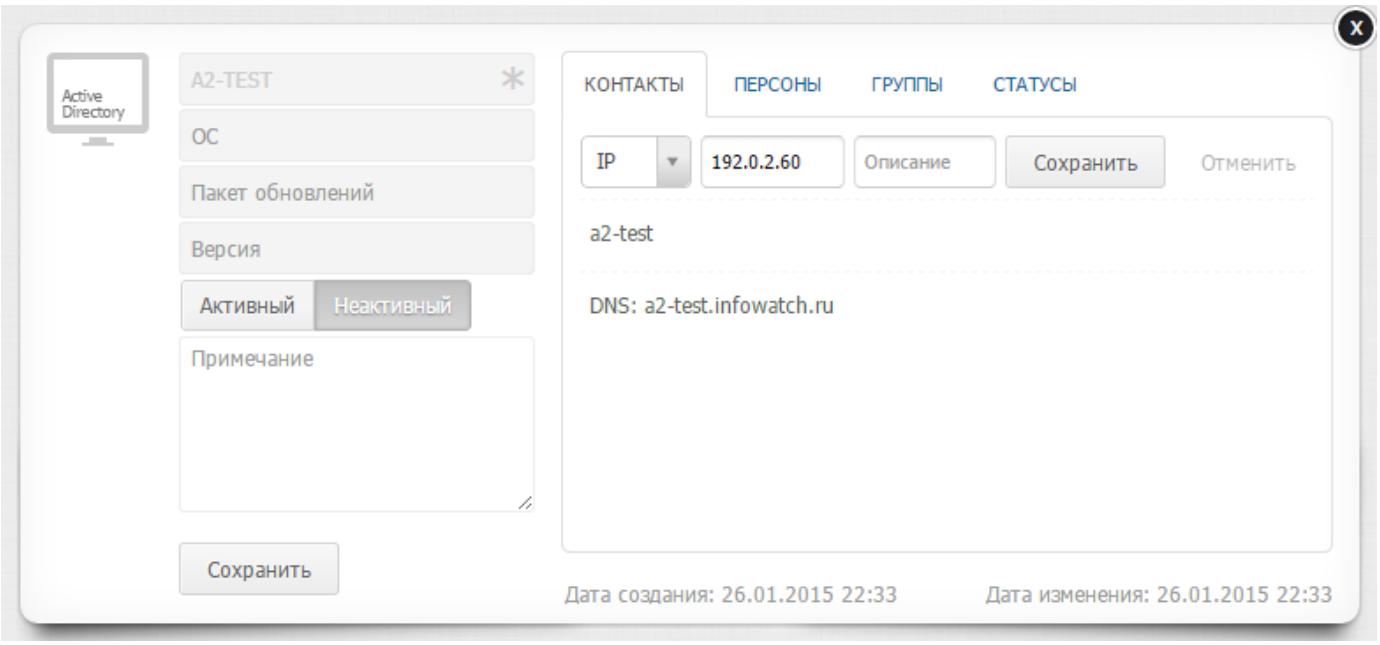
Целевые действия пользователя:

- Работа с группами персон (см. "Создание группы персон и рабочих станций")
- Просмотр виджетов с информацией о персонах (см. "Просмотр сводки по персоне/рабочей станции")
- Создание фильтра по персонам (см. "Просмотр событий по персоне/рабочей станции")
- Настройка карточки персоны ("Настройка карточки персоны")
- Формирование политики для персон (см. "Добавление персоны/рабочей станции в политику")
- Работа со статусами персон (см. "Добавление статуса персоне/рабочей станции")
- Добавлены персоны в периметр (см. "Добавление персоны/рабочей станции в периметр компании")

4.6.3 Рабочие станции



Пример списка рабочих станций



Пример диалога редактирования рабочей станции

Атрибуты рабочей станции:

Параметр	Описание
Имя	Наименование рабочей станции
Примечание	Произвольное описание

Параметр	Описание
Контакты	Идентификатор рабочей станции в сети: • IP • DNS В первом из двух полей необходимо указать IP или DNS-имя (в зависимости от выбранной настройки). Во втором поле, если необходимо, оставьте свой комментарий.
Персоны	Персоны, к учетным записям которых привязана рабочая станция
Группы	Группы, включающие рабочую станцию
Статус	Статус, который офицер безопасности назначает рабочей станции

Целевые действия пользователя:

- Работа с группами рабочих станций (см. "Создание группы персон и рабочих станций")
- Работа с рабочими станциями (см. "Создание списка персон и рабочих станций")
- Просмотр виджетов с информацией о рабочих станциях (см. "Просмотр сводки по персоне/рабочей станции")
- Создание фильтра по рабочим станциям (см. "Просмотр событий по персоне/рабочей станции")
- Формирование политики для рабочих станций (см. "Добавление персоны/рабочей станции в политику")
- Работа со статусами рабочих станций (см. "Добавление статуса персоне/рабочей станции")
- Определение рабочих станций, входящих в периметры (см. "Добавление персоны/рабочей станции в периметр компании")

4.7 Раздел "Политики"

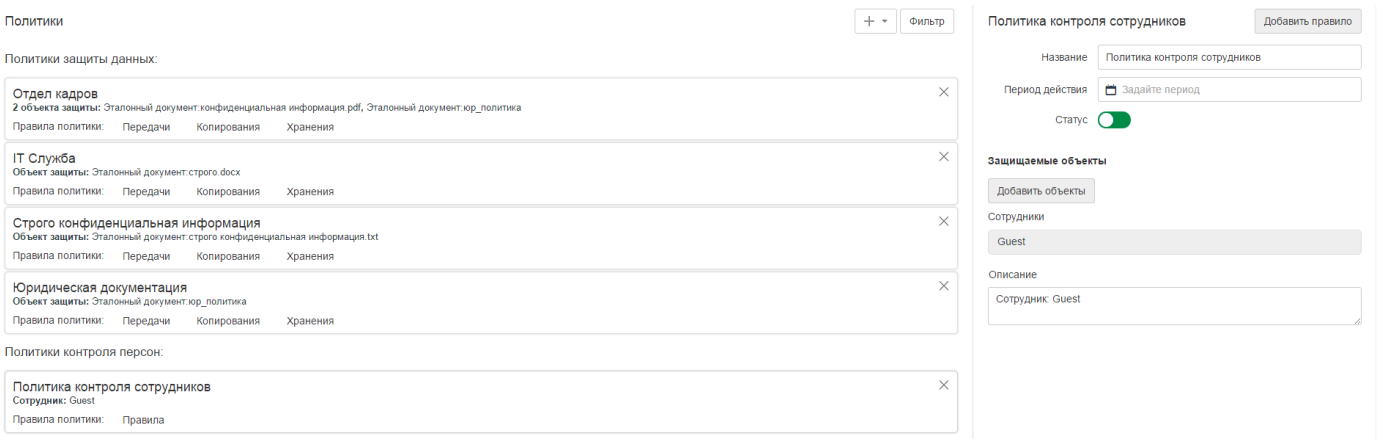
Справочная информация:
Политики - совокупность *правил*, в соответствии с которыми проводится анализ и обработка объектов перехвата. ***Правило*** состоит из набора условий, по которым выполняется проверка объекта, и действий, осуществляемых при выполнении или невыполнении заданных условий.

Важно!

В результате анализа Система не будет производить никаких действий, если выполняется хотя бы одно из следующих условий:

- в Системе нет ни одной политики;
- все имеющиеся в Системе политики неактивны;
- ни одна имеющаяся в Системе политика не имеет активных правил (или действия по умолчанию для активных политик не определены).

О разделе:
Раздел содержит список действий, которые выполняет Система в ответ на действия персон и рабочих станций.



В разделе содержатся следующие элементы:

Элемент	Назначение
Список политик	Содержит доступные политики. Политики в списке разделены на две группы: политики защиты данных и политики контроля персон.
Форма просмотра политики	Содержит атрибуты выбранной политики
Форма просмотра правила	Позволяет настроить правило для выбранной политики
Кнопка **Фильтр**	Отображает область **Настройка фильтра**
Область **Настройка фильтра**	Позволяет отфильтровать политики по указанным атрибутам
Кнопка добавления политики 	Позволяет выбрать тип политики в раскрывающемся списке. Доступные значения: • Политика защиты данных • Политика контроля персон Для добавленной политики в правой части рабочей области отображается форма ее просмотра
Форма просмотра политики	Позволяет указать параметры созданной политики

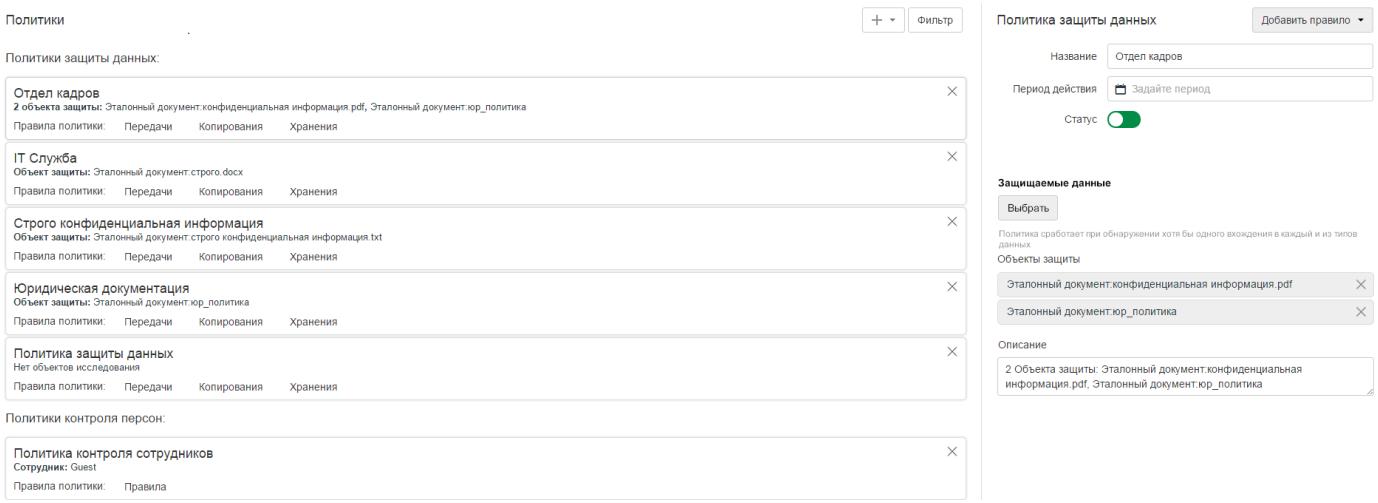
Целевые действия пользователя:

- Добавление новой политики (см. "Создание политики защиты данных" и "Создание политики контроля персон")
- Изменение ранее созданной политики (см. "Редактирование политики")
- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")

- Фильтрация политик (см. "Фильтрация списка политик")

4.7.1 Политики и форма их просмотра

Форма просмотра политики отображается в правой части рабочей области при выборе политики в списке.



Атрибуты политик:

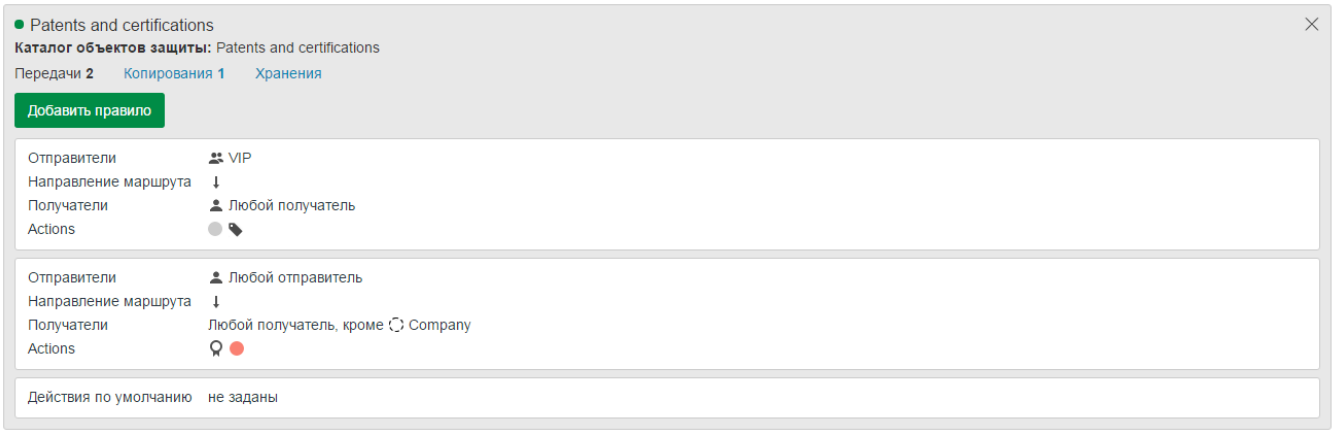
Параметр	Описание
Название	Название политики
Статус	Показатель того, активна ли политика в Системе
Период действия	Временной промежуток, в который действует политика
Защищаемые данные (только для политики защиты данных)	Список объектов защиты, их каталогов и файловых форматов, контроллируемых политикой
Контроллируемые персоны (только для политики контроля персон)	Список персон, действия которых контроллируются политикой
Правила политики	Список действий, выполняемых Системой при срабатывании политики
Описание	Описание политики. Необязательный параметр.

Целевые действия пользователя:

- Добавление новой политики (см. "Создание политики защиты данных" и "Создание политики контроля персон")
- Изменение ранее созданной политики (см. "Редактирование политики")

4.7.2 Правила и форма их просмотра

Информация о правилах указывается в плитке политики, для которой они определены. При нажатии на ссылку с типом правил в плитке политики раскрывается список добавленных правил этого типа.



При выборе правила в списке в правой части рабочей области отображается форма просмотра выбранного правила.

Также в правом верхнем углу плитки правила отображается значок ×, нажав на который вы можете удалить выбранное правило.

Для **политики защиты данных** существуют три категории правил:

Правило	Описание
Правило передачи	Правило, регулирующее отправку и получение защищаемых данных
Правило копирования	Правило, регулирующее копирование, печать и фотосъемку защищаемых данных
Правило хранения	Правило, регулирующее хранение защищаемых данных

При создании правил передачи и копирования для выбора LDAP-домена в качестве *Отправителя* или *Получателя* необходимо предварительно настроить синхронизацию с LDAP-сервером и добавить домен через закладку **Группы**.

Также для *Отправителя* и *Получателя* можно указать следующие параметры:

Параметр	Описание

Параметр	Описание
Контакты	Укажите контакты отправителей/получателей трафика. Для этого в выпадающем списке слева выберите тип контакта:  - аккаунт ICQ. Целое число от 10000 до 999999999999;  - аккаунт Skype. Строка от 6 до 32 символов, должна начинаться с буквы; может содержать только латинские буквы, цифры и символы «.», «,», «-», «_»);  - номер мобильного телефона. Строка от 3 символов, может содержать только цифры, пробел и символы "-","_", "( )","+",".");  - номер стационарного телефона. Строка от 3 символов, может содержать только цифры, пробел и символы "-","_", "( )","+",".");  - адрес электронной почты. Адрес в формате RFC;  - адрес электронной почты Lotus. Строка от 3 символов при вводе данных в поле ввода или строка от 1 символа при вводе данных в окне **Отправители** (открывается при нажатии кнопки );  - идентификатор на Web-ресурсе. Строка от 3 символов при вводе данных в поле ввода или строка от 1 символа при вводе данных в окне **Отправители** (открывается при нажатии кнопки ).
Группы	Укажите группы, члены которых являются отправителями/получателями трафика.
Персоны	Укажите персон, которые являются отправителями/получателями трафика.
Домены	Укажите домены, члены которых являются отправителями/получателями трафика.
Периметры	Укажите периметры, элементы которых являются отправителями/получателями трафика.

Правила контроля персон регулируют действия контролируемых персон, а также позволяют применить к выбранным персонам имеющиеся в Системе политики защиты данных.

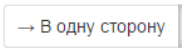
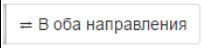
Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")

4.7.2.1 Правило передачи

Атрибуты правила передачи:

Параметр	Описание

Параметр	Описание
Направление маршрута	Направления могут быть двух типов:  - правило срабатывает только в случае передачи трафика от отправителя получателю;  - правило срабатывает при передаче трафика от отправителя получателю и от получателя отправителю.
Тип события	Тип трафика, передача которого, при выполнении прочих настроек, приводит к срабатыванию правила. Возможные варианты: • Веб-сообщение • Email • Веб-почта • ICQ • XMPP • Mail.ru Агент • Jabber • Skype • MS Lync • Yahoo! • WhatsApp • SMS • Фотосъемка
Дни недели действия правила	Список дней недели, в которые правило будет срабатывать
Время действия правила в течение дня	Интервал времени в сутках, в который правило будет срабатывать
Компьютеры	Рабочие станции отправителя
Отправители	Список персон и рабочих станций, передача трафика которыми, при выполнении прочих настроек: - приводит к срабатыванию правила  - не приводит к срабатыванию правила

Параметр	Описание
Получатели	Список персон и рабочих станций, получение трафика которыми, при выполнении прочих настроек:  - приводит к срабатыванию правила  - не приводит к срабатыванию правила **Примечание.** Если в качестве защищаемых данных указан объект защиты на базе графического объекта и выбран тип события **Веб-почта**, то для срабатывания политики требуется не указывать персон в поле **Получатели**. Данное ограничение связано с тем, что в событиях веб-почты получателем вложения считается домен. Например, если письмо с вложением отправлено на адрес `user1@example.com`, то получателем вложения будет считаться домен `example.com`. Такие образом, если в качестве получателей указаны определенные персоны, то событие, содержащее во вложении графический объект, не попадет под действие политики.
Отправить уведомление	Список пользователей Консоли управления, которым будет отправлено уведомление в случае срабатывания правила **Примечание:** Если после создания правила пользователь или его e-mail будут удалены из Системы (о работе с учетными записями пользователей см. *"Руководство администратора"*, раздел "Пользователи"), то уведомление данному пользователю отправлено не будет.
Уведомить отправителя	Включите эту настройку, чтобы в случае срабатывания правила отправителям трафика было выслано уведомление. По умолчанию данная настройка отключена.
Назначить вердикт	Вердикт, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Разрешить*, *Заблокировать*, *Поместить на карантин.*
Назначить уровень нарушения	Уровень нарушения, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
Теги	Список тегов, которые будут назначены объекту в случае срабатывания правила (см. "Теги")
Назначить персонам статус	Статус, который будет назначен отправителям в случае срабатывания правила (см. "Статусы")
Удалить событие	Если выбрана данная опция, то событие не будет сохранено в базу данных, а также не будут выполнены действия, заданные в правиле. По умолчанию данная настройка отключена.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")

- Добавление действий в политику (см. "Определение действий Системы в случае нарушения правил")

4.7.2.2 Правило копирования

Атрибуты правила копирования:

Параметр	Описание
Тип события	Тип трафика, копирование которого, при выполнении прочих настроек, приводит к срабатыванию правила. Возможные варианты: • Копирование на внешнее устройство • FTP • Печать • Фотосъемка
Дни недели действия правила	Список дней недели, в которые правило будет срабатывать
Часы действия правила	Интервал времени в сутках, в который правило будет срабатывать
Рабочие станции	Список рабочих станций, передача трафика которыми, при выполнении прочих настроек, приводит к срабатыванию правила
Отправители	Список персон и рабочих станций, передача трафика которыми, при выполнении прочих настроек: - приводит к срабатыванию правила  - не приводит к срабатыванию правила
Отправить уведомление	Список пользователей Консоли управления, которым будет отправлено уведомление в случае срабатывания правила **Примечание:** Если после создания правила пользователь или его e-mail будут удалены из Системы (о работе с учетными записями пользователей см. *"Руководство администратора"*, раздел "Пользователи "), то уведомление данному пользователю отправлено не будет.
Назначить уровень нарушения	Уровень нарушения, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*
Теги	Список тегов, которые будут назначены объекту в случае срабатывания правила (см. "Теги")
Назначить персонам статус	Статус, который будет назначен отправителям в случае срабатывания правила (см. "Статусы")
Удалить событие	Если выбрана данная настройка, то событие не будет сохранено в базу данных, а также не будут выполнены действия, заданные в правиле. По умолчанию данная настройка отключена.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")
- Добавление действий в политику (см. "Определение действий Системы в случае нарушения правил")

4.7.2.3 Правило хранения

Атрибуты правила хранения:

Параметр	Описание
Тип события	Тип трафика, хранение которого, при выполнении прочих настроек, приводит к срабатыванию правила. Возможные варианты: • Краулер
Место хранения	Список мест, хранение защищаемых объектов в которых: - приводит к срабатыванию правила  - не приводит к срабатыванию правила **Примечание:** При добавлении сетевого ресурса используйте следующий формат записи: `//<workstation>/<directory>` где: • `<workstation>` - название рабочей станции; • `<directory>` - целевая папка на рабочей станции. При добавлении файлового хранилища введите следующие значения в поля: • в поле **Введите источник** - адрес сервера базы данных SharePoint; • в поле **Введите путь хранения** - имя экземпляра базы данных SharePoint.
Владельцы файла	Обнаружение защищаемых данных у указанных персон и групп, а также внутри указанных периметров приводит к срабатыванию правила. При отрицании атрибута правило сработает при обнаружении защищаемых данных у любых владельцев, за исключением указанных персон и групп, а также за пределами указанных периметров.
Кому доступен файл	Доступность файла указанным персонам, группам персон, а также в пределах указанных периметров приводит к срабатыванию правила. При отрицании атрибута правило сработает в случае доступности файла персонам и группам, за исключением указанных, а также за пределами указанных периметров.

Параметр	Описание
Отправить уведомление	Список пользователей Консоли управления, которым будет отправлено уведомление в случае срабатывания правила **Примечание:** Если после создания правила пользователь или его e-mail будут удалены из Системы (о работе с учетными записями пользователей см. *"Руководство администратора"*, раздел "Пользователи "), то уведомление данному пользователю отправлено не будет.
Назначить уровень нарушения	Уровень нарушения, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*
Теги	Список тегов, которые будут назначены объекту в случае срабатывания правила (см. "Теги")
Назначить персонам статус	Статус, который будет назначен отправителям в случае срабатывания правила (см. "Статусы")
Удалить событие	Если выбрана данная настройка, то событие не будет сохранено в базу данных, а также не будут выполнены действия, заданные в правиле. По умолчанию данная настройка отключена.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")
- Добавление действий в политику (см. "Определение действий Системы в случае нарушения правил")

4.7.2.4 Правило контроля персон

Атрибуты правила контроля персон:

Параметр	Описание
Перехватывать с уровнем нарушения	Будет выполняться перехват событий с заданным уровнем нарушения
Связать с политикой	Политики защиты данных, срабатывание которых будет инициировать срабатывание правила (при условии, что уровень нарушения соответствует значению поля **Перехватывать с уровнем нарушения**)
Отправить уведомление	Список пользователей Консоли управления, которым будет отправлено уведомление в случае срабатывания правила **Примечание:** Если после создания правила пользователь или его e-mail будут удалены из Системы (о работе с учетными записями пользователей см. *"Руководство администратора"*, раздел "Пользователи"), то уведомление данному пользователю отправлено не будет.
Уведомить отправителя	Включите эту настройку, чтобы в случае срабатывания правила отправителям трафика было выслано уведомление. По умолчанию данная настройка отключена.

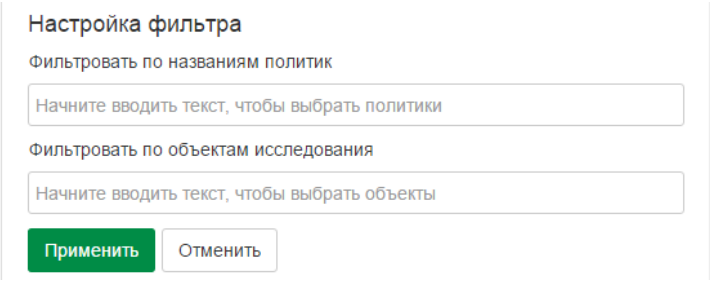
Параметр	Описание
Назначить вердикт	Вердикт, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Разрешить*, *Заблокировать*, *Поместить на карантин.*
Назначить уровень нарушения	Уровень нарушения, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
Теги	Список тегов, которые будут назначены объекту в случае срабатывания правила (см, "Теги")
Удалить событие	Если выбрана данная настройка, то событие не будет сохранено в базу данных, а также не будут выполнены действия, заданные в правиле. По умолчанию данная настройка отключена.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")
- Добавление действий в политику (см. "Определение действий Системы в случае нарушения правил")

4.7.3 Область "Настройка фильтра"

Отображается при нажатии на кнопку **Фильтр** в разделе **Политики**.



Атрибуты фильтра:

Параметр	Описание
Фильтровать по названиям политик	Фильтрация выполняется с учетом указанных политик
Фильтровать по объектам	Фильтрация выполняется с учетом указанных защищаемых данных

Целевые действия пользователя:

- Фильтрация политик (см. "Фильтрация списка политик")

4.7.4 Окно добавления политики

Атрибуты политик описаны в статье "Политики и область их просмотра". При создании новой политики вы можете указать защищаемые данные (для политики защиты данных) и контролируемых персон (для политики контроля персон).

Содержимое области добавления политики различается в зависимости от выбранного типа:

Тип политики	Описание области добавления политики
Политика защиты данных	При выборе новая политика добавляется в список политик защиты данных, а в правой части рабочей области отображается область просмотра политики. При нажатии на кнопку **Выбрать объекты** открывается диалоговое окно, в котором вы можете указать защищаемые данные, входящие в одну из следующих категорий: • Каталог объектов защиты • Объекты защиты • Файловый формат
Политика контроля персон	При выборе открывается диалоговое окно, в котором требуется указать отправителей, действия которых будут контролироваться данной политикой. Вы можете выбрать отдельных персон, группу персон или персон, объединенных общим статусом.

Целевые действия пользователя:

- Добавление новой политики (см. "Создание политики защиты данных" и "Создание политики контроля персон")

4.8 Раздел "Списки"

Справочная информация:
Списки - наборы однотипных данных, создаваемые средствами Консоли управления, или предустановленные, для использования при составлении политик.

О разделе:
Раздел содержит редактируемые справочники тегов, ресурсов, статусов, периметров и файлов.



Раздел **Списки**, вкладка **Статусы**

В разделе содержатся следующие элементы:

Элемент	Назначение

Элемент	Назначение
Вкладки различных типов справочников • Теги • Список ресурсов • Статусы • Периметры • Список файлов	Содержат списки элементов и инструменты для выбранного справочника
Список элементов или групп элементов для выбранного справочника	Открывается при выборе справочника. Содержит список элементов справочника или группу списков элементов справочника
Панель навигации по страницам	Набор кнопок для просмотра страниц, содержащих записи (в случае, если не все записи помещаются на одной странице)
Панель инструментов	Набор инструментов для справочников

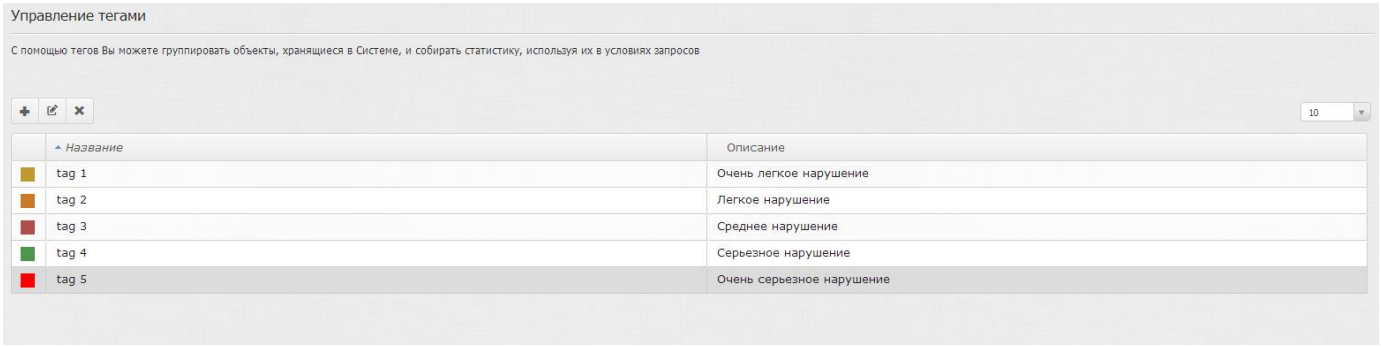
Целевые действия пользователя:

- Формирование списка тегов (см. "Работа с тегами")
- Формирование списка ресурсов (см. "Работа со списком ресурсов")
- Формирование списка статусов (см. "Работа со статусами")
- Формирование периметров (см. "Работа с периметрами")
- Включение файловых форматов в политику ("Создание политики защиты данных")

4.8.1 Теги

Справочная информация:

Тег - метка, дающая краткую характеристику перехваченному объекту.



Атрибуты тегов:

Параметр	Описание
Цвет	Цветовой маркер, устанавливаемый вместе с тегом
Название	Название тега

Параметр	Описание
Описание	Примечание в произвольной форме

В Системе существуют следующие предустановленные теги:

- **Защита от удаления** - события, которые не будут удалены при освобождении пространства в базе данных;

> **Примечание:**
>
> Данный тег доступен только для версии Traffic Monitor Standard на базе Oracle Standard (подробнее см. "*Infowatch Traffic Monitor. Руководство администратора*").

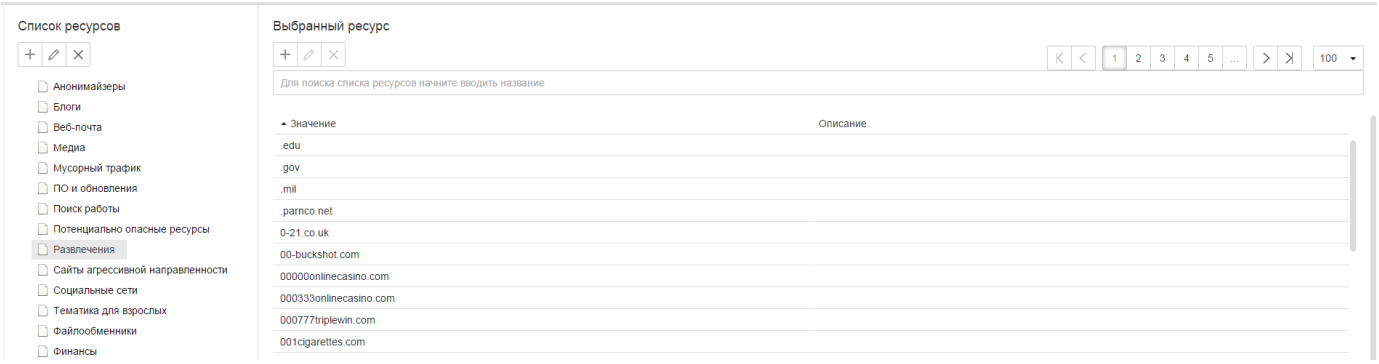
- **На рассмотрение** - события, характеризующие подозрительную активность персон;
- **VIP** - события, инициированные руководством организации.

Целевые действия пользователя:

- Формирование списка тегов (см. "Работа с тегами")

4.8.2 Список ресурсов

Справочная информация:
Список ресурсов - набор Интернет-ресурсов, посещение которых детектируется Системой как нецелевое использование рабочего времени.



Ресурсы организованы в списки в соответствии с их тематикой.

Атрибуты ресурсов описаны в таблице:

Параметр	Описание
Значение	Наименование ресурса в сети Интернет
Описание	Произвольное примечание

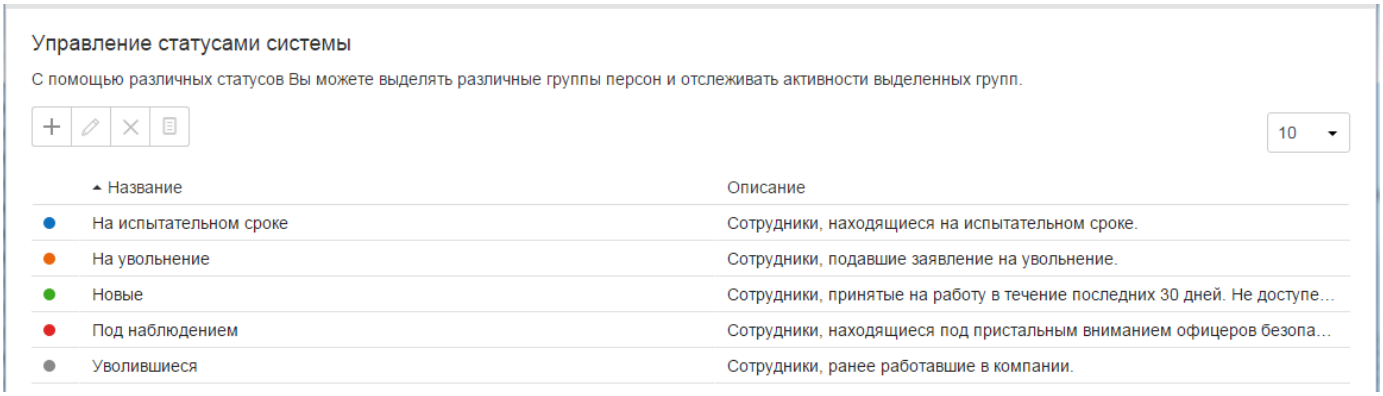
Целевые действия пользователя:

- Формирование списка ресурсов (см. "Работа со списком ресурсов")

4.8.3 Статусы

Справочная информация:
Статус персоны - метка, созданная одним из следующих способов:

- автоматически присвоена персоне в соответствии со статусом персоны или рабочей станции, импортированных из Active Directory;
- вручную присвоена персоне офицером безопасности;
- автоматически назначена отправителю в результате срабатывания правила.



Статусы *На испытательном сроке*, *На увольнение*, *Новый*, *Под наблюдением* и *Уволившиеся* являются предустановленными.

Примечание.

Статус *Новый* не доступен для удаления.

Атрибуты статуса персоны:

Параметр	Описание
Цвет	Цветовой маркер, добавляемый вместе со статусом
Название	Название статуса
Описание	Описание статуса. Необязательный параметр

Целевые действия пользователя:

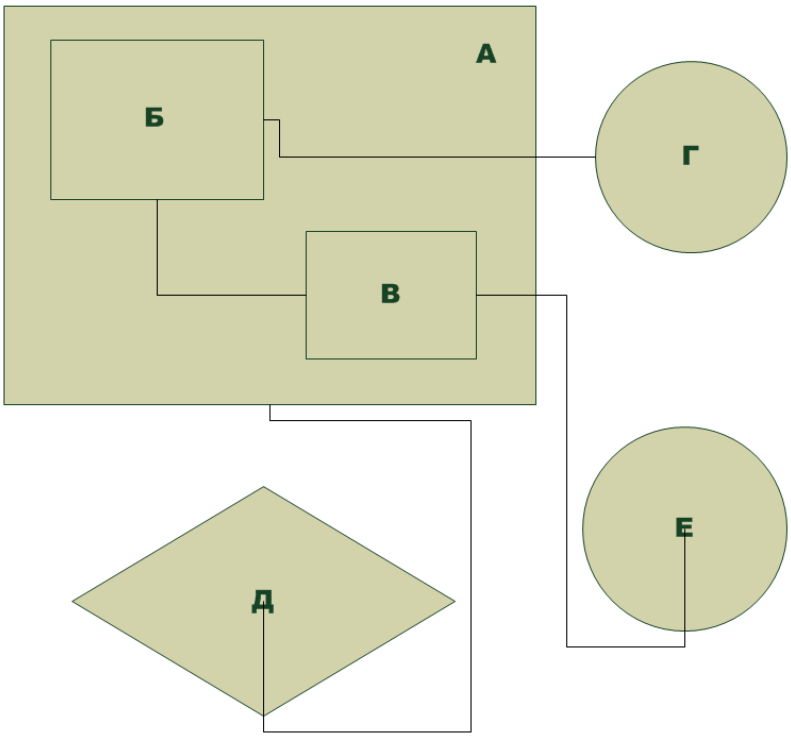
- Формирование списка статусов (см. "Работа со статусами")
- Ручное назначение статуса персоне или рабочей станции для отслеживания активности, а также для визуального отличия (см. "Добавление статуса персоне")
- Автоматическое назначение статуса отправителю в случае срабатывания правила (см. "Правила и форма их просмотра", атрибут **Назначить отправителю статус**)
- При добавлении политики контроля персон - выбор в качестве объектов исследования персон с определенными статусами (см. "Создание политики контроля персон")

4.8.4 Периметры

Справочная информация:
Периметр - это контейнер, содержащий элементы инфраструктуры компании (сотрудников, домен и прочие) и контактные данные. Периметр используется для того, чтобы логически разделить организацию на структурные элементы и следить за трафиком каждого из таких элементов.

Например:

- Есть компания с инфраструктурой А, в которой есть подразделения Б и В;
- Компания взаимодействует с организациями Г, Д и Е.

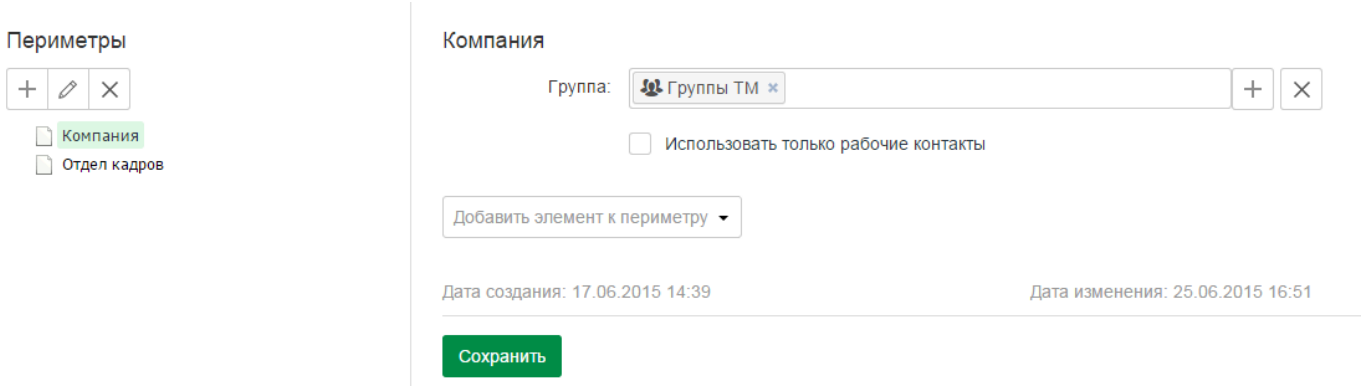


Выделив в периметры все названные объекты (А, Б, В, Г, Д, Е), офицер безопасности может настроить контроль трафика:

- внутри компании (в пределах периметра А);
- за пределами компании (между периметром А и одним из периметров Г, Д или Е).

Важно!

Для более гибкой работы со структурными элементами рекомендуется выделять меньшие периметры в больших (в приведенном примере - периметры Б и В в периметре А).



Атрибуты периметра:

Параметр	Описание
Название	Наименование периметра
Список элементов	Входящие в периметр элементы **Важно!** При добавлении в периметр персон или групп доступна функция **Использовать только рабочие контакты**. Вы можете использовать эту функцию, например, для того, чтобы отправка сотрудником сообщения с личного почтового ящика не считалась передачей данных за периметр.
Дата создания	Дата и время создания периметра
Дата изменения	Дата и время последнего редактирования периметра

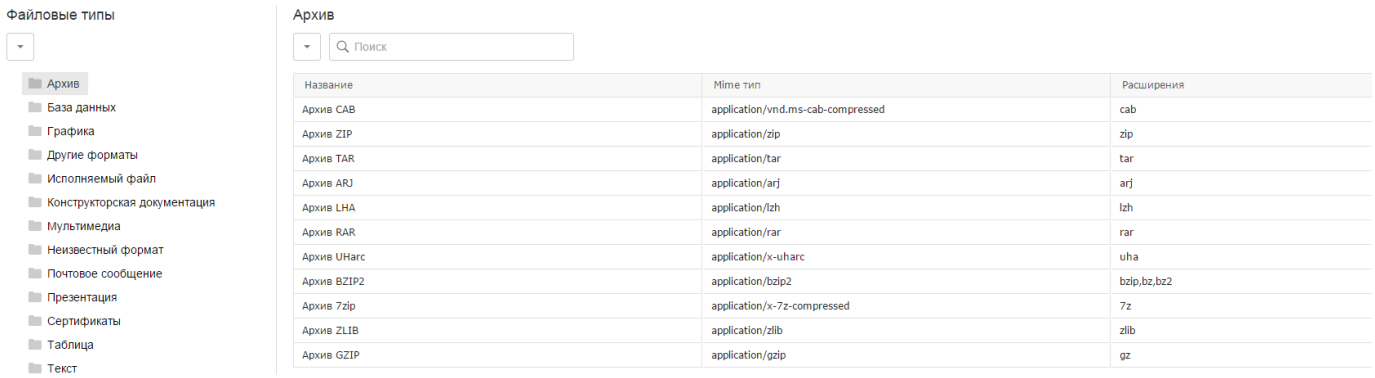
Целевые действия пользователя:

- Формирование периметров (см. "Работа с периметрами")

4.8.5 Список файлов

Справочная информация:

Список файлов - набор типов файлов, которые детектируются в Системе.



Файлы различных форматов разделены на группы в зависимости от предметной области. Например, тип **Архив** содержит файлы с расширением ZIP, RAR и прочие.

На вкладке содержатся следующие элементы:

Элемент	Назначение
Список типов файлов	Расположен в левой части рабочей области. Содержит набор предметных областей, в которых используются файлы одного или нескольких форматов.
Список форматов файлов выбранного типа	Расположен в правой части рабочей области. Содержит список атрибутов всех файлов данного типа, которые детектируются в Системе. Представляет собой таблицу, которая содержит в себе описание **Названия**, **Mime типа** и **Расширения**.
Кнопка **Создать политику**	Создание политики защиты данных, в качестве защищаемого объекта для которой указан выбранный формат файлов или тип файлов **Примечание:** После нажатия на кнопку открывается форма добавления новой политики в разделе **Политики**

Важно!

Списки файлов строго определены Системой и недоступны для изменения.

Целевые действия пользователя:

- Работа с политиками (см. "Создание политики защиты данных")

4.9 Раздел "Краулер"

Справочная информация:
Подсистема ***Краулер*** системы InfoWatch Traffic Monitor позволяет выполнять проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративных политик безопасности. Таким образом InfoWatch Crawler позволяет контролировать файловые ресурсы компании для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

Краулер обеспечивает выполнение следующих функций:

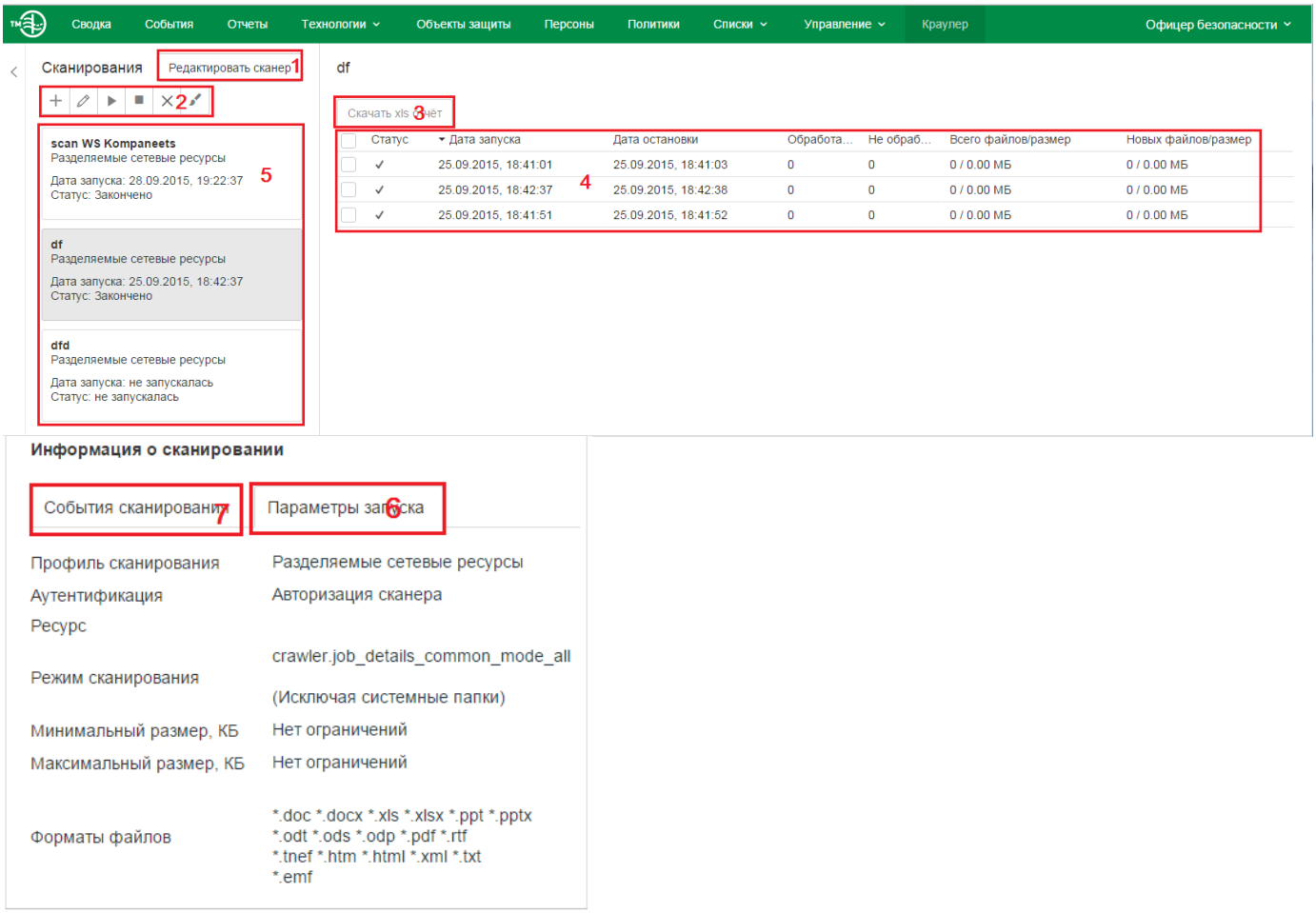
- Сканирование сетевых папок, открытых для удалённого доступа по протоколу SMB.
- Сканирование локальных дисков рабочих станций, работающих под управлением ОС Windows.
- Сканирование файлового хранилища SharePoint. Выполняет проверку документов, хранящихся в БД Microsoft SharePoint 2007/2010/2013. При этом рассматриваются только текущие версии файлов: история изменений не исследуется.
- Пользовательская настройка параметров сканирования: скорость загрузки файлов со сканируемых ресурсов и параметры файловой очереди для загрузки объектов на сервер Traffic Monitor.
- Создание задания сканирования с возможностью указывать:
    - перечень папок и сетевых узлов, на которых будет выполняться сканирование;
    - маски обрабатываемых файлов;

  - ограничения по размеру обрабатываемых файлов;
  - расписание выполнения задания (также возможен ручной запуск).
- Отбор только новых и измененных файлов: ранее обработанные файлы повторно на сервер InfoWatch Traffic Monitor не отправляются.
- Передача файлов для анализа на сервер InfoWatch Traffic Monitor с заданными пользователем параметрами передачи.
- Сохранение файлов согласно настройкам политики (по умолчанию – инцидентов: файлов, признанных потенциальным нарушением действующей политики безопасности)
- Представление результатов сканирования в Консоли управления: с помощью запросов на просмотр объектов и в виде отчётов, в том числе предустановленных.

Краулер не выполняет удаления, перемещения, переименования, шифрования или каких-либо иных действий над файлами – даже в тех случаях, когда они признаны потенциальным нарушением. Происходит только информирование офицера безопасности о наличии инцидента: из Консоли управления InfoWatch Traffic Monitor доступен просмотр файлов, признанных потенциальным нарушением, с указанием подробной информации об их расположении и пользователях, имеющих к нему доступ.

Работа с подсистемой Краулер ведется в Консоли управления InfoWatch Traffic Monitor, в разделе **Краулер**.

О разделе:
Раздел содержит средства для создания, редактирования и запуска задач для подсистемы Краулер.



В разделе содержатся следующие элементы:

№ на схеме	Элемент	Назначение
1	Кнопка редактирования сканера	При нажатии, в правой части рабочей области отображается форма редактирования сканера
2	Панель инструментов	Набор инструментов для заданий сканирования
3	Кнопка **Скачать xls отчет** (см. "Сохранение отчета")	Позволяет сохранить отчет о выполнении задания в формате XLS
4	Поле просмотра истории запусков задания на сканирование (см. "История запусков")	Содержит сведения об этапах выполнения задания на сканирование
5	Список заданий на сканирование (см. "Задание на сканирование")	Содержит список задач сканирования для выбранного сканера
6	Вкладка "Параметры запуска"	Содержит данные о выбранном задании на сканирование
7	Вкладка "События сканирования"	Содержит данные о событиях сканирования: дату и время возникновения события и сообщение с содержанием события

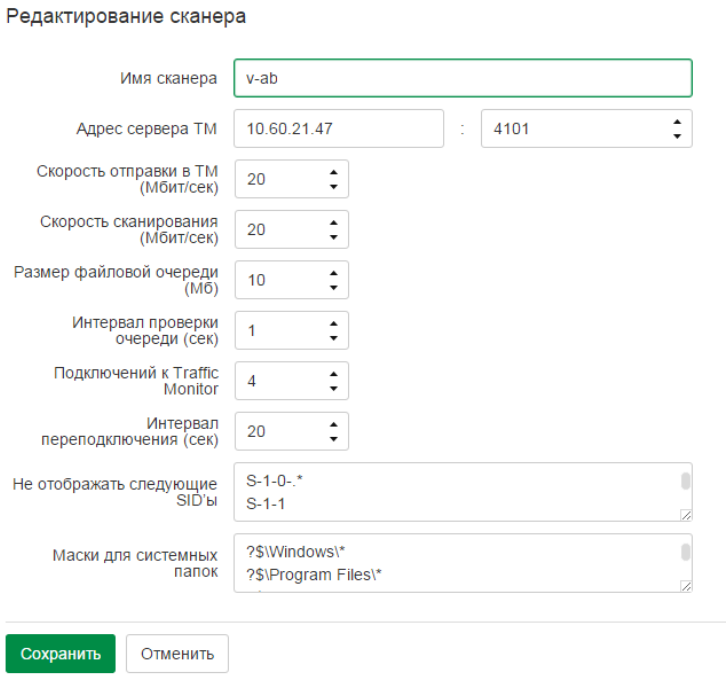
Целевые действия пользователя:

- Редактирование установленных в Системе сканеров (см. "Настройка сканера")
- Формирование задачи на сканирование (см. "Создание задачи")
- Запуск и остановка задачи на сканирование (см. "Запуск и остановка задачи")
- Изменение задачи на сканирование (см. "Редактирование задачи")
- Очистка хеша задачи на сканирование (см. "Очистка хешей")
- Просмотр истории задачи на сканирование (см. "Просмотр истории запусков")
- Сохранение на жесткий диск отчета о выполнении задачи на сканирование (см. "Сохранение отчета")

4.9.1 Сканер

Справочная информация:
Сканер - модуль подсистемы Краулер, выполняющий сканирование мест хранения информации (хранилище Microsoft SharePoint 2007/2010/2013, локальные диски рабочих станций, разделяемые сетевые ресурсы), определенных пользователем с помощью заданий на сканирование.

> **Примечание:**
>
> При сканировании хранилища SharePoint необходимо, чтобы Сканер находился с ним в одном домене.



Атрибуты сканера:

Параметр	Описание
Имя сканера	Название сканера
Адрес сервера ТМ	IP-адрес сервера Traffic Monitor, где работает служба `iw_expressd`
Скорость отправки в ТМ (Мбит/сек)	Максимальная скорость загрузки файлов на сервер Traffic Monitor, Мбит/с Позволяет снизить нагрузку на сервер Traffic Monitor при большом количестве передаваемых файлов
Скорость сканирования (Мбит/сек)	Максимальная скорость загрузки файлов с проверяемых ресурсов во временное хранилище, Мбит/с Позволяет снизить нагрузку на рабочую станцию, на которой производится сканирование
Размер файловой очереди (Мб)	Максимальный суммарный размер очереди, куда помещаются найденные файлы перед отправкой на сервер Traffic Monitor, Мбайт **Важно!** При достижении максимального суммарного размера задания останавливаются, и все файлы из этого буфера удаляются без отправки в Traffic Monitor.
Интервал проверки очереди (сек)	Интервал (в секундах), с которым сервер Crawler будет проверять наличие объектов в очереди для загрузки на сервер Traffic Monitor. Если в очереди есть хотя бы один объект, он будет передан на сервер Traffic Monitor
Подключений к Traffic Monitor	Максимальное количество одновременных подключений к серверу Traffic Monitor
Интервал переподключения (сек)	Интервал (в секундах), с которым сервер Crawler будет пытаться восстановить подключение к серверу Traffic Monitor в случае потери подключения
Не отображать следующие SID'ы	Позволяет настроить фильтр персон
Маски для системных папок	Маски папок, которые не будут сканироваться при работе сканера

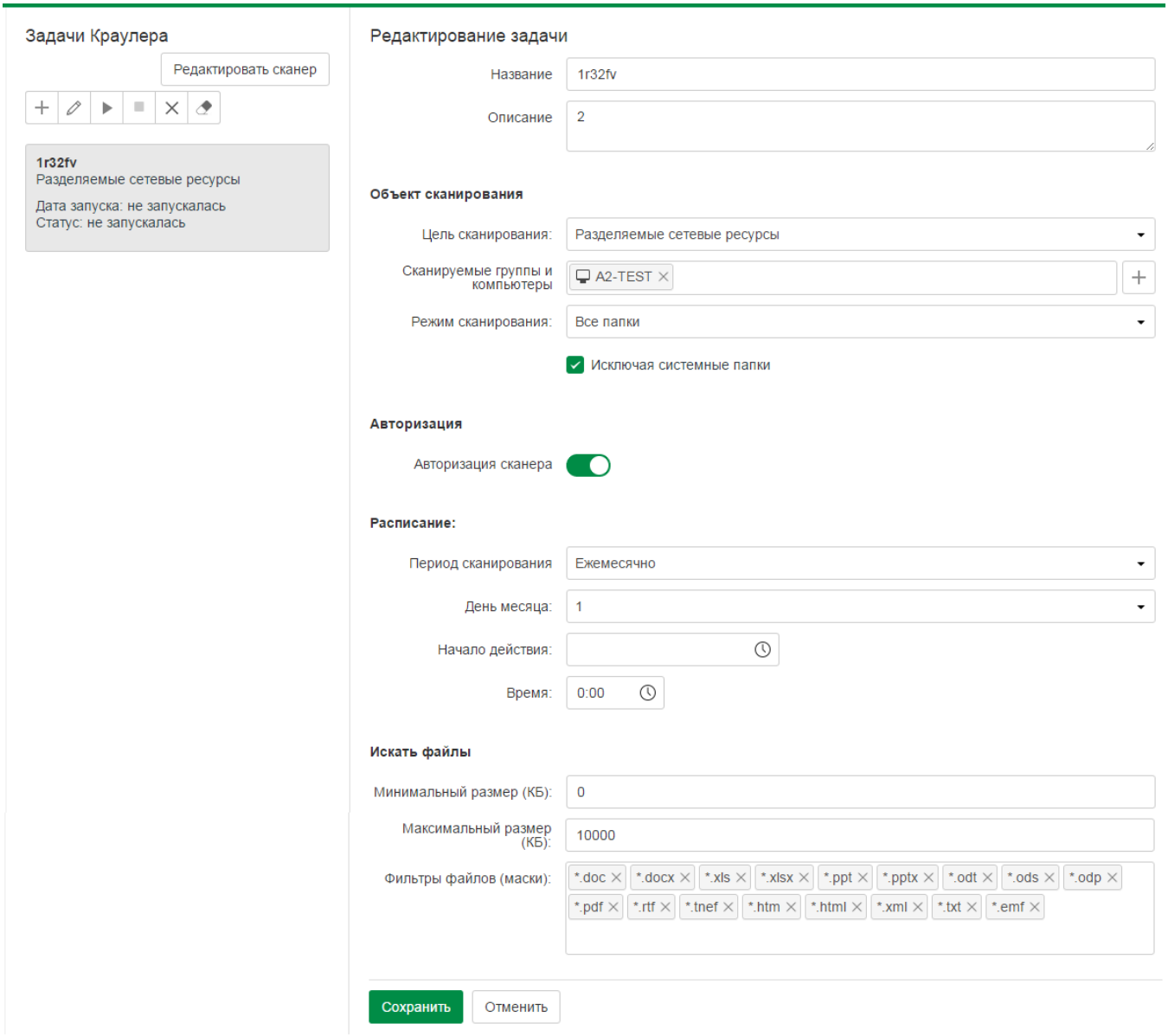
Целевые действия пользователя:

- Редактирование установленных в Системе сканеров (см. "Настройка сканера")
- Формирование задачи на сканирование (см. "Создание задачи")
- Запуск и остановка задачи на сканирование (см. "Запуск и остановка задачи")
- Изменение задачи на сканирование (см. "Редактирование задачи")
- Очистка хеша задачи на сканирование (см. "Очистка хешей")
- Просмотр истории задачи на сканирование (см. "Просмотр истории запусков")
- Сохранение на жесткий диск отчета о выполнении задачи на сканирование (см. "Сохранение отчета")

4.9.2 Задание на сканирование

Справочная информация:
Задание на сканирование - единичная или повторяющаяся по расписанию операция проверки

целевых мест хранения информации (хранилище Microsoft SharePoint 2007/2010/2013, локальные диски рабочих станций, разделяемые сетевые ресурсы) на предмет хранения конфиденциальных данных (подробнее о списке конфиденциальных данных см. "Определение конфиденциальной информации"). Атрибуты задания отображаются при переходе в режим редактирования.



Задание на сканирование и форма его редактирования

Атрибуты задания:

Параметр	**Описание**
Название	Наименование задания
Описание	Произвольное примечание

Цель сканирования	Тип задачи сканирования: • **Разделяемые сетевые ресурсы** • **Локальные диски рабочих станций** При использовании политики **Локальные диски рабочих станций** необходимо, чтобы на рабочих станциях с Windows XP была отключена настройка **Use simple file sharing** (**Control Panel -> Folder Options**, вкладка **View**) • **Файловое хранилище SharePoint** В зависимости от используемой версии SharePoint указываются следующие параметры: **Для SharePoint 2007 и 2010:** ○ **Версия SharePoint** - используемая версия SharePoint: 2007 или 2010; ○ **Адрес БД ресурса** - адрес сервера базы данных SharePoint. Например, sharepoint-test; ○ **Название БД ресурса** - имя экземпляра базы данных SharePoint. Например, wss_content. **Для SharePoint 2013:** ○ **Версия SharePoint** - используемая версия SharePoint: 2013; ○ **Адрес SharePoint сервера** - адрес сервера базы данных SharePoint, указывается с учетом протокола http:// или https://.
Сканируемые группы и компьютеры	Группы персон и рабочие станции, подлежащие сканированию

Режим сканирования	**Все папки** - сканирует все папки на рабочей станции **Все папки, кроме** - сканирует все папки на рабочей станции с установленными исключениями **Только папки** - сканирует только папки, указанные пользователем **Примечание:** Если требуется сканировать в том числе системные папки, снимите флажок в поле **Исключить системные папки**. По умолчанию сканирование системных папок не выполняется. **Для написания пути сканирования используются следующие символы:** * - 0 и более любых символов ? - один любой символ $ - символ, который используется Windows для указания скрытой папки **Важно!** В конце пути сканирования должен быть указан символ ***** либо ****. Например, путь может иметь следующий вид: "C?\folder*" или "C?\folder\". **При сканировании разделяемого ресурса или хранилища SharePoint, можно использовать следующие запросы:** Docs* - будет сканировать папку Docs и все подпапки. пример текста - будет искать словосочетание "пример текста" в пути. .формат файла - будет сканировать файлы указанного формата (.txt) **При сканирование локальных дисков и папок, можно использовать следующие запросы:** C$\Docs* - будет сканировать папку Docs и все подпапки на диске C: *\Docs* - будет сканировать папку Docs и все подпапки вне зависимости от их расположения. ?$\Docs* - будет сканировать любую папку, имя которой имеет 1 символ и папку Docs со всеми подпапками. (C$\Docs\, D$\Docs) \Docs????* - будет сканировать любую папку, которая имеет имя Docs с четырьмя дополнительными символами (Docs1234) **Важно!** В режиме сканирования **Все папки** сканирование будет происходить только для локальных дисков рабочей станции.
Авторизация	Вы можете использовать авторизацию сканера (в этом случае сканирования будет выполняться под учетной записью, от имени которой запущен сканер) либо указать логин и пароль учетной записи вручную. По умолчанию используется авторизация сканера. **Важно!** При сканировании хранилища SharePoint должен быть указан пользователь сервера MS SQL, на котором расположена целевая БД. **Важно!** Краулер использует доступ к контроллеру домена для получения информации о пользователе или группе по уникальному идентификатору (SID). Для обеспечения доступа учетная запись должна быть доменной и иметь права на чтение ресурса, который предполагается сканировать.
Период сканирования	Расписание, согласно которому производится сканирование **Важно!** Если выбран период **Ежемесячно**, то для запуска задания на сканирование необходимо, чтобы текущий месяц содержал дату, указанную в качестве значения параметра **День месяца**. Например, если выбрано значение 30, то в феврале сканирование запускаться не будет.

Минимальный размер (Кб)	Минимальный размер сканируемых файлов в килобайтах
Максимальный размер (Кб)	Максимальный размер сканируемых файлов в килобайтах
Фильтры файлов (маски)	Расширения сканируемых файлов. **Чтобы добавить новый формат:** 1. В поле со списком форматов введите требуемое расширение и нажмите клавишу **Enter**. 2. Введенное значение добавится в список форматов. 3. Чтобы удалить какое-либо значение, нажмите на крестик рядом с требуемым форматом.

Целевые действия пользователя:

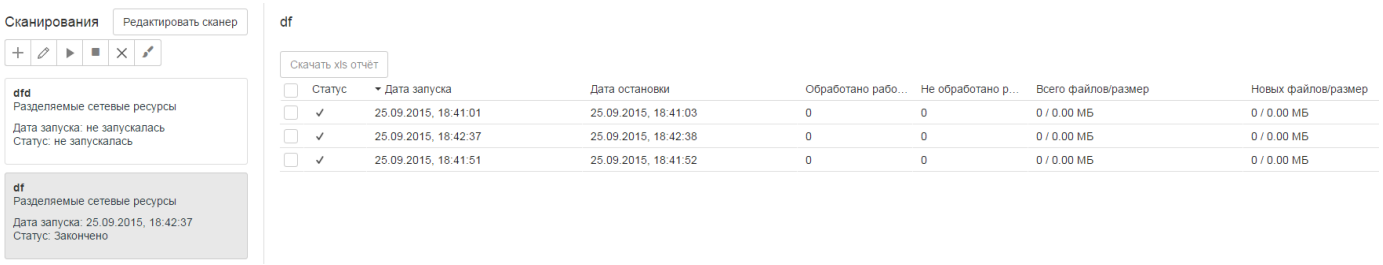
- Формирование задачи на сканирование (см. "Создание задачи")
- Запуск и остановка задачи на сканирование (см. "Запуск и остановка задачи")
- Изменение задачи на сканирование (см. "Редактирование задачи")
- Очистка хеша задачи на сканирование (см. "Очистка хешей")
- Просмотр истории задачи на сканирование (см. "Просмотр истории запусков")
- Сохранение на жесткий диск отчета о выполнении задачи на сканирование (см. "Сохранение отчета")

4.9.3 История запусков

Справочная информация:
В правой части рабочей области отображается информация о запусках выбранного задания на сканирование.

При выборе одной из записей в таблице открывается подробная информация о выбранном запуске, размещенная на вкладках:

- **События сканирования** - вкладка содержит системные сведения о запуске задания на сканирование;
- **Параметры запуска** - вкладка содержит список атрибутов задания на сканирование (см. "Задание на сканирование").



Задание на сканирование и форма его просмотра

Атрибуты задания описаны в таблице:

Параметр	Описание
Статус	Идентификатор статуса задания (- *Запущено*, - *Остановлено*, - *Выполнено*)
Дата запуска	Дата и время запусков задания
Дата остановки	Дата и время остановок задания
Обработано рабочих станций	Количество целевых рабочих станций, обработанных за время выполнения задания
Не обработано рабочих станций	Количество целевых рабочих станций, не обработанных за время выполнения задания
Всего файлов/размер	Количество файлов на целевых рабочих станциях, обработанных за время выполнения задания/размер файлов
Новых файлов/размер	Количество ранее не обрабатываемых файлов на целевых рабочих станциях, за время выполнения задания/размер файлов

Целевые действия пользователя:

- Просмотр информации об этапах выполнения задания на сканирование (см. "Просмотр истории запусков")

5 РЕШЕНИЕ ЗАДАЧ

Работа Офицера безопасности в Консоли управления сводится к следующим основным задачам:

- Работа с персонами и рабочими станциями;
- Работа со справочниками;
- Работа с базой технологий;
- Работа с объектами защиты;
- Работа с подсистемой Краулер;
- Работа с объектами перехвата;
- Настройка реакций Системы;
- Работа с отчетами.

Однотипные действия, выполняемые в рамках перечисленных задач, описаны в разделе "Типовые действия".

Важно!

Администрирование Консоли управление выходит за рамки полномочий Офицера безопасности и в данном документе не описывается. Вы можете найти необходимую информацию в документе «*Infowatch Traffic Monitor. Руководство администратора*».

Об элементах интерфейса в разделах Консоли управления читайте:

- Раздел Сводка
- Раздел События
- Раздел "Отчеты"
- Раздел Технологии
- Раздел Объекты защиты
- Раздел Персоны
- Раздел Политики
- Раздел Списки
- Раздел Краулер

5.1 Типовые действия

Для чего требуются типовые действия:
Для выполнения однотипных операций во время использования Консоли управления.

К типовым действиям относятся следующие операции:

Операция	Описание
Вход в Консоль управления и выход из нее	Порядок авторизации в Консоли управления и порядок выхода из Консоли управления
Применение конфигурации Системы	Внесенные в конфигурацию Системы изменения вступают в силу с момента применения конфигурации
Редактирование элемента	Вы можете выполнять настройку сущностей, необходимые для настройки конфигурации Системы, отображения и обработки объектов перехвата
Удаление элемента	Вы можете удалять из интерфейса сущности, которые использовались для настройки конфигурации Системы, отображения и обработки объектов перехвата
Навигация по страницам	Вы можете просматривать большие количества элементов в многостраничном режиме: для перехода к конкретной странице с элементами используются кнопки навигации
Изменение пароля пользователя	Порядок смены пользователем Консоли управления собственного пароля
Выбор языка интерфейса	Порядок изменения языка интерфейса Консоли управления
Вызов справки	Обращение к справочной информации
Просмотр сведений о Системе	Вызов общей информации о Системе

5.1.1 Вход в Консоль управления и выход из нее

Цель:

1. Войти в Консоль управления.
2. Выйти из Консоли управления.

Решение:

1. **Чтобы войти в Консоль управления:**
    a. Откройте интернет-браузер Google Chrome версии 30 или выше (если указанный браузер не установлен, вы можете загрузить его, перейдя по ссылке).
    b. Перейдите по адресу, выданному Вам системным администратором. В окне браузера отобразится стартовая страница Консоли управления.
    c. В поле **Логин** укажите имя пользователя.
    d. В поле **Пароль** укажите пароль.
    Примечание:
    Логин и пароль Вы можете получить у администратора InfoWatch Traffic Monitor.
    e. Нажмите **Войти**.
2. **Чтобы выйти из Консоли управления:**
    a. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления").

b. Выберите **Выйти**.

5.1.2 Применение конфигурации Системы

Справочная информация:
В конфигурацию Системы включено содержимое следующих разделов Консоли управления:

- Технологии
- Объекты защиты
- Персоны
- Политики
- Списки

По завершении редактирования элементов этих разделов необходимо применить сделанные изменения, чтобы они вступили в действие: то есть Система начала бы работать в соответствии с внесенными изменениями

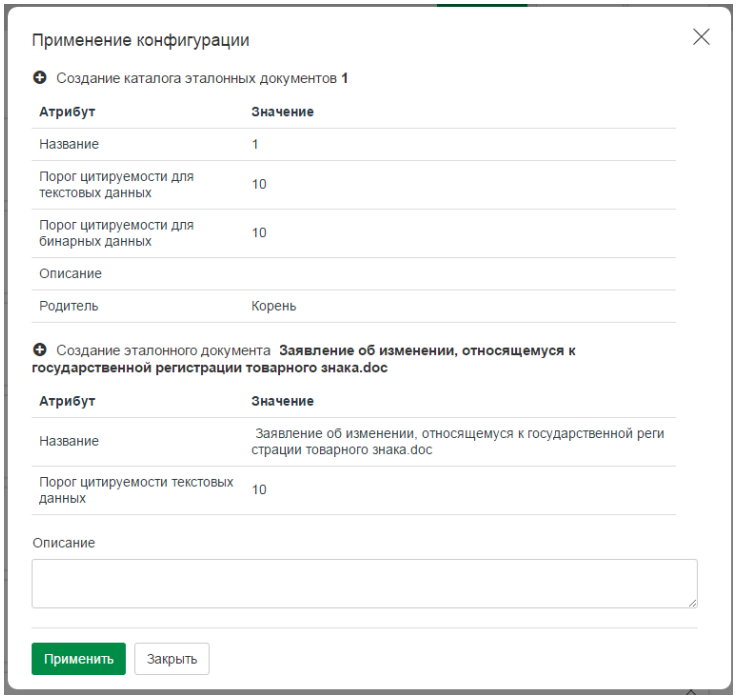
Цель:
Применить конфигурацию Системы.

Решение:

1. По окончании редактирования конфигурации в верхней части окна браузера нажмите **Применить** на строке вида:



Откроется окно **Применение изменений конфигурации**, содержащее информацию о внесенных изменениях:



2. При необходимости введите текст в поле **Описание**.

3. Нажмите **Применить**.

5.1.3 Редактирование элемента

Цель:
Изменить атрибуты ранее созданного элемента.

Решение:

1. Перейдите в целевой раздел.
2. При необходимости перейдите в целевой подраздел или на целевую вкладку.
3. Для редактирования целевого элемента выделите его в списке с помощью левой кнопки мыши (либо выберите элемент в раскрывающемся списке) и нажмите **Редактировать**.
4. Введите требуемые атрибуты элемента (атрибуты всех элементов описаны в статье "Интерфейс Консоли управления").
5. Нажмите **Сохранить**.

5.1.4 Удаление элемента

Цель:
Удалить элемент.

Решение:

1. Перейдите в целевой раздел.
2. При необходимости перейдите в целевой подраздел или на целевую вкладку.
3. Для удаления целевого элемента щелчком левой кнопки мыши выделите его из списка (либо выберите в раскрывающемся списке).

> **Примечание:**
>
> Вы можете удалить несколько элементов списка, при выделении удерживая клавишу *Shift* или *Ctrl*.

4. Нажмите **Удалить**.
5. В окне подтверждения удаления нажмите **Да**.

5.1.5 Навигация по страницам

Справочная информация:
Навигация по страницам может осуществляться только в многостраничном режиме просмотра элементов интерфейса.

Многостраничный режим просмотра используется для более эргономичного использования рабочей области и доступен, когда в окне браузера отображается панель навигации по страницам:



Панель навигации по страницам

Цель:
Перейти к требуемой странице в многостраничном режиме.

Решение:

1. Перейдите в целевой раздел.
2. При необходимости перейдите в целевой подраздел или на целевую вкладку.
3. В раскрывающемся списке, расположенном в правой части панели навигации, укажите, какое количество элементов должно отображаться на странице.
4. Для навигации по страницам используйте кнопки с номерами страниц, содержащих элементы. Вы также можете использовать кнопки:
    - **|<** - для перехода на первую страницу;
    - **<** - для перехода на предыдущую страницу;
    - **>** - для перехода на следующую страницу;
    - **>|** - для перехода на последнюю страницу.

Примечание:

При использовании сортировки списка кнопки навигации работают в соответствии с обновленным списком.
Например, при сортировке списка, начинающегося на "А", кнопка **>|** переведет на страницу, содержащую элементы на "Я". Но при обратной сортировке кнопка **>|** переведет на страницу, содержащую элементы на "А".

5.1.6 Изменение пароля пользователя

Справочная информация:
Пользователь может изменить пароль учетной записи, от имени которой он авторизован в Системе, воспользовавшись специальной функцией.

Цель:
Изменить пароль пользователя.

Решение:

1. Нажмите на кнопку меню пользователя и выберите пункт **Сменить пароль**.
   На экран будет выведено диалоговое окно **Смена пароля**.
2. В открывшемся диалоговом окне введите пароль, который будет назначен учетной записи, в поля:
    - **Пароль**;
    - **Подтверждение пароля**.

Примечание:

Подробные рекомендации по составлению паролей см. в документе «*Infowatch Traffic Monitor. Руководство администратора*».

3. Нажмите **Сохранить**.

5.1.7 Выбор языка интерфейса

Цель:
Изменить язык интерфейса Консоли управления.

Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления") и в блоке **Сменить язык** выберите требуемый язык.
2. В открывшемся диалоговом окне **Изменение языка** нажмите **Да**.

Вернуть русский язык можно аналогичным способом: с той разницей, что названия будут отображаться на выбранном языке интерфейса.

5.1.8 Вызов справки

Цель:
Получить справочную информацию о работе в Системе.
Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления") и выберите **Помощь**.
   В новой вкладке браузера отобразится руководство пользователя InfoWatch Traffic Monitor.
2. Ознакомьтесь с информацией, после чего закройте вкладку стандартным способом.

5.1.9 Просмотр сведений о Системе

Цель:
Получить справочную информацию о Системе.

Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления") и выберите **О Системе**.
   На экран будет выведено окно **О Системе**, в котором будут отображаться сведения об используемой версии Системы.
2. Ознакомьтесь с информацией, после чего закройте окно стандартным способом.

5.2 Работа с персонами и рабочими станциями

Для чего требуется работа с персонами и рабочими станциями:
Наличие списков персон и рабочих станций облегчает офицеру безопасности работу с перехваченными объектами. Это происходит за счет учета информации об отправителях и получателях (персонах), а также рабочих станциях с помощью специальных справочников.

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Работа с персонами и рабочими станциями состоит из следующих действий:

Действие	Описание
Создание группы персон и рабочих станций	Создание структурного элемента справочника
Создание списка персон и рабочих станций	Наполнение справочника
Просмотр сводки по персоне/рабочей станции	Настройка виджетов для отображения статистической информации по персоне/рабочей станции
Просмотр событий по персоне/рабочей станции	Просмотр объектов перехвата для требуемой персоны/рабочей станции
Добавление статуса персоне/рабочей станции	Выделение персоны/рабочей станции особым маркером для отслеживания активности, а также для визуального отличия
Добавление персоны/рабочей станции в периметр компании	Внесение персоны/рабочей станции в установленные списки компании
Настройка карточки персоны	Наполнение данными записи о персоне
Настройка карточки рабочей станции	Наполнение данными записи о рабочей станции

См. также:

- "Раздел Персоны" - о разделе, в котором ведется работа со списками персон и рабочих станций

5.2.1 Создание группы персон и рабочих станций

Цель:
Создать группу персон и рабочих станций.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выберите **Группы ТМ**.
3. На панели инструментов в левой части рабочей области нажмите **Создать группу**.
4. Укажите атрибуты новой группы (см. "Группы персон и рабочих станций").
5. Нажмите **Да**.

> **Важно**
>
> При создании новой группы события для этой группы будут отображаться, начиная с момента применения конфигурации.

Вы можете добавить в группу ТМ имеющиеся группы Active Directory. В этом случае при добавлении/удалении пользователей в группе Active Directory состав соответствующей группы Traffic Monitor обновится автоматически.

Чтобы добавить группу Active Directory в группу Traffic Monitor, выделите в списке групп нужную группу Active Directory с помощью мыши и, удерживая левую клавишу мыши зажатой, перетащите выбранный элемент в требуемую группу Traffic Monitor.
В одну группу Traffic Monitor можно добавить группы из различных доменов. Таким же способом можно добавить в группу ТМ отдельных пользователей из домена.

> **Примечание**
>
> Для того чтобы состав групп Traffic Monitor, содержащих группы Active Directory, обновлялся автоматически, необходимо выполнить синхронизацию с LDAP-сервером.

О наполнении созданных групп смотрите "Создание персон и рабочих станций".

Дополнительные сведения:

Редактирование и удаление групп персон и рабочих станций выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.2.2 Создание персон и рабочих станций

Справочная информация:
Список персон и рабочих станций может наполняться двумя способами:

- из каталога Active Directory компании - настраивается администратором Системы (см. документ «*Infowatch Traffic Monitor. Руководство администратора*»);
- средствами Traffic Monitor - формируется офицером безопасности, как описано в этом подразделе.

Цель:
Наполнить группу персон и рабочих станций.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку:
    - **Персоны** - чтобы добавить персону;
    - **Рабочие станции** - чтобы добавить рабочую станцию.
4. На панели инструментов в правой части рабочей области нажмите **Добавить**.
5. Укажите характеристики новой персоны или рабочей станции (см. "Персоны" и "Рабочие станции").
6. Нажмите **Сохранить**.

Дополнительные сведения:
Редактирование и удаление персон и рабочих станций выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.2.3 Просмотр событий по персоне

Цель:
Просматривать события по персоне или рабочей станции.

Решение:

1. Создайте запрос, указав в параметрах запроса целевую персону (подробнее см. "Создание запросов").
2. Выполните созданный запрос.

Аналогичным способом выполняется просмотр событий по рабочей станции.

Пример:
Если требуется, чтобы были показаны все объекты перехвата за текущую неделю, отправителем которых был *Иванов* (подразумевается, что персона *Иванов* создана в разделе **Персоны** до начала интересующего периода):

1. Офицер безопасности переходит в раздел **События** и создает запрос с названием *Иванов*, указав следующие значения:
    - атрибуту **Дата перехвата** - значение *Текущая неделя*;
    - атрибуту **Отправители** - значение *Иванов* (выбирает из списка ранее созданных персон).
2. Офицер безопасности сохраняет и выполняет созданный запрос.

В результате отобразится список, содержащий все найденные события.

5.2.4 Просмотр сводки по персоне

Цель:
Просматривать статистические данные по персоне или рабочей станции.

Решение:

1. Создать запрос, указав в параметрах запроса целевую персону (см. "Фильтрация событий").
2. Создайте виджет **Подборка**, указав в атрибуте **Подборка** ранее созданный запрос (см. "Создание виджета")

Аналогичным способом выполняется просмотр сводки по рабочей станции.

Пример:
Если требуется, чтобы были показаны все объекты перехвата за текущую неделю, отправителем трафика в которых был *Иванов* (подразумевается, что персона *Иванов* уже создана в разделе **Персоны**):

1. Офицер безопасности переходит в раздел **Сводка**
2. Офицер безопасности создает виджет с названием *Иванов*, причем атрибуту **Подборка** указывает ранее созданный запрос *Иванов* (см. "Просмотр событий по персоне").
3. Офицер безопасности сохраняет созданный виджет.

В разделе **Сводка** на виджете *Иванов* отображаются все требуемые события.

5.2.5 Добавление статуса персонам

Цель:
Добавить статус персоне или рабочей станции.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку:
   - **Персоны** - чтобы добавить статус персоне;
   - **Рабочие станции** - чтобы добавить статус рабочей станции.
4. Выделите целевую персону или целевую рабочую станцию.
5. На панели инструментов в правой части рабочей области нажмите и в раскрывающемся списке выберите **Назначить статус**.
6. В открывшемся диалоговом окне укажите требуемый статус и при необходимости введите описание.
7. Нажмите **Сохранить**.

Примечание:

Статус *Новый* присваивается персоне и рабочей станции в момент создания в Системе и сохраняется в течение 30 дней (в случае импорта персон и рабочих станций из Active Directory статус *Новый* сохраняется в течение 30 дней с момента создания записей в Active

Directory).

См. также:

- "Статусы" - о подразделе, в котором ведется работа со статусами персон.

5.2.6 Добавление персоны в периметр

Цель:
Добавить персону или группу в существующий периметр.

Решение:

1. Перейдите в раздел **Списки**->**Периметры**.
2. Щелчком левой кнопки мыши выберите целевой периметр из списка периметров (см. "Периметры").
3. В правой части рабочей области нажмите **Добавить элемент к периметру** и в раскрывающемся списке выберите **Персона**.
4. В появившемся поле **Персона** укажите целевую персону одним из следующих способов:
   - начните вводить имя или фамилию и выберите из раскрывающемся списка необходимую запись;
   - нажмите + **Добавить**, в открывшемся диалоговом окне установите флажок в поле с целевой персоной (вы можете указать несколько персон) и нажмите **Сохранить**.
5. В области редактирования периметра нажмите **Сохранить**.

Аналогичным способом выполняется добавление в периметр группы персон.

Пример:

Если требуется, чтобы в периметр *Бухгалтерия* входила группа *Финансисты*:

Офицер безопасности выделяет периметр *Бухгалтерия* в списке периметров. Далее ОБ добавляет группу *Финансисты*:

1. нажимает **Добавить элемент к периметру**;
2. в раскрывающемся списке выбирает **Группа персон**;
3. в поле **Группа персон** указывает *Финансисты* и нажимает **Сохранить**.

См. также:

- "Периметры" - о подразделе, в котором ведется работа с периметрами.

5.2.7 Настройка карточки персоны

Цель:

Наполнить данными карточку персоны.

Настройка карточки персоны состоит из следующих действий:

Действие	Описание
Добавление персоне контакта	Добавление контактных данных для созданной персоны
Добавление персоне рабочей станции	Добавить рабочую станцию, связанную с персоной
Добавление персоны в группу	Добавление персоны в имеющуюся группу

5.2.7.1 Добавление персоне контакта

Цель:
Добавить или отредактировать контактные данные персоны.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевую запись;
   - щелчком левой кнопки мыши выделите целевую запись и на панели инструментов нажмите **Редактировать**.

   Откроется форма редактирования карточки персоны.
4. В правой части формы редактирования карточки персон перейдите на вкладку **Контакты**.
5. Нажмите **Добавить контакт** и укажите требуемые параметры:
   - тип контакта: электронная почта, электронная почта Lotus, мобильный телефон, стационарный телефон, Skype, ICQ, Web-контакт;
   - является ли контакт личным или рабочим;
   - значение (адрес или номер) контакта;
   - произвольное описание.
6. Нажмите **Сохранить**.

Примечание.

Значение контакта необходимо указывать в следующем формате:

- - мобильный телефон (строка от 3 символов; может содержать только цифры, пробел, и символы: "-","_", "( )","+");
- - стационарный телефон (строка от 3 символов; может содержать только цифры, пробел, и символы: "-","_", "( )","+");
- - e-mail (адрес электронной почты в формате RFC);

- - контакт Skype (строка от 1 символа);
- - контакт ICQ (строка от 1 символа);
- - WEB-идентификатор, например, профиль в социальной сети (строка от 1 символа);
- - электронная почта Lotus (строка от 1 символа).

Чтобы отредактировать ранее указанные контактные данные:

1. Выделите нужный контакт с помощью левой клавиши мыши и на панели инструментов нажмите .
2. Отредактируйте параметры контакта.
3. Нажмите **Сохранить**.

5.2.7.2 Добавление персоне рабочей станции

Цель:
Добавить персоне связанную рабочую станцию.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевую запись;
   - щелчком левой кнопки мыши выделите целевую запись и на панели инструментов нажмите **Редактировать**.

   Откроется форма редактирования карточки персоны.
4. В правой части формы редактирования карточки персоны перейдите на вкладку **Компьютеры**.
5. Нажмите **Добавить рабочую станцию**.
6. В открывшемся окне установите флажки в полях напротив требуемых рабочих станций и нажмите **Да**.
7. Нажмите **Сохранить**.

5.2.7.3 Добавление персоны в группу

Цель:
Добавить персону в имеющуюся группу.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевую запись;
   - щелчком левой кнопки мыши выделите целевую запись и на панели инструментов в правой части рабочей области нажмите **Редактировать персону**.

   Откроется форма редактирования карточки персоны.
4. В правой части формы редактирования карточки персоны перейдите на вкладку **Группы**.
5. Нажмите **Добавить группу**.
6. В открывшемся окне установите флажок напротив требуемых группы и нажмите **Добавить**.
7. Нажмите **Сохранить**.

Если требуется удалить персону из текущей группы:

1. Выделите требуемую персону на вкладке **Персоны**.
2. На панели инструментов в правой части рабочей области нажмите и в раскрывающемся списке нажмите **Покинуть текущую группу**.
3. В открывшемся окне подтверждения нажмите **Да**.

> **Важно!**
>
> Если персона состоит только в одной группе, то при выполнении этой команды персона будет удалена.

5.2.8 Настройка карточки компьютера

Цель:
Наполнить данными карточку компьютера.

Настройка карточки компьютера состоит из следующих действий:

Действие	Описание
Добавление компьютеру контакта	Добавление компьютеру контакта IP/DNS или доменного аккаунта
Добавление персоны для компьютера	Добавление персоны, связанной с данным компьютером
Добавление компьютера в группу	Добавление компьютера в имеющуюся группу

5.2.8.1 Добавление компьютеру контакта

Цель:
Указать для компьютера IP-адрес, DNS-имя или доменный аккаунт.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевую рабочую станцию;
   - щелчком левой кнопки мыши выделите целевую рабочую станцию и на панели инструментов нажмите **Редактировать**.

   Откроется форма редактирования карточки компьютера.
4. В правой части формы редактирования карточки компьютера перейдите на вкладку **Контакты**.
5. Нажмите **Добавить контакт** и укажите требуемые параметры:
   - тип контакта: **IP**, **DNS** или **Доменный аккаунт**;
   - значение контакта: адрес IP, имя DNS или название доменного аккаунта;
   - произвольное описание.
6. Нажмите **Сохранить**.

5.2.8.2 Добавление компьютеру персоны

Цель:
Добавить персоне связанный компьютер.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевой компьютер;
   - щелчком левой кнопки мыши выделите целевой компьютер и на панели инструментов нажмите **Редактировать**.

   Откроется форма редактирования карточки компьютера.
4. В правой части формы редактирования карточки компьютера перейдите на вкладку **Персоны**.
5. Нажмите **Добавить персону**.
6. В открывшемся окне установите флажки в полях напротив требуемых персон и нажмите **Сохранить**.

7. Нажмите **Сохранить** на форме редактирования.

Для удаления добавленной персоны выделите ее в списке и нажмите ×.

5.2.8.3 Добавление компьютера в группу

Цель:
Добавить компьютер в имеющуюся группу.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевой компьютер;
   - щелчком левой кнопки мыши выделите целевой компьютер и на панели инструментов нажмите

     Редактировать.

   Откроется форма редактирования карточки компьютера.
4. В правой части формы редактирования карточки рабочей станции перейдите на вкладку **Группы**.
5. Нажмите  **Добавить группу**.
6. В открывшемся окне установите флажки в полях напротив требуемых групп и нажмите **Добавить**.
7. Нажмите **Сохранить**.

Если требуется удалить компьютер из текущей группы:

1. Выделите требуемый компьютер на вкладке **Компьютеры**.
2. На панели инструментов в правой части рабочей области нажмите

   и в раскрывающемся списке нажмите **Покинуть текущую группу**.
3. В открывшемся окне подтверждения нажмите **Да**.

> **Важно!**
>
> Если компьютер состоит только в одной группе, то при выполнении этой команды он будет удален.

5.3 Работа со справочниками

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Для чего требуется работа со справочниками:
Для того чтобы добавлять, редактировать или удалять справочники, используемые в Системе.

Работа со справочниками состоит из следующих действий:

Действие	Описание
Работа с тегами	Редактирование списка меток
Работа со списком ресурсов	Редактирование списка ресурсов.
Работа со статусами	Редактирование списка статусов
Работа с периметрами	Редактирование списка периметров

См. также:

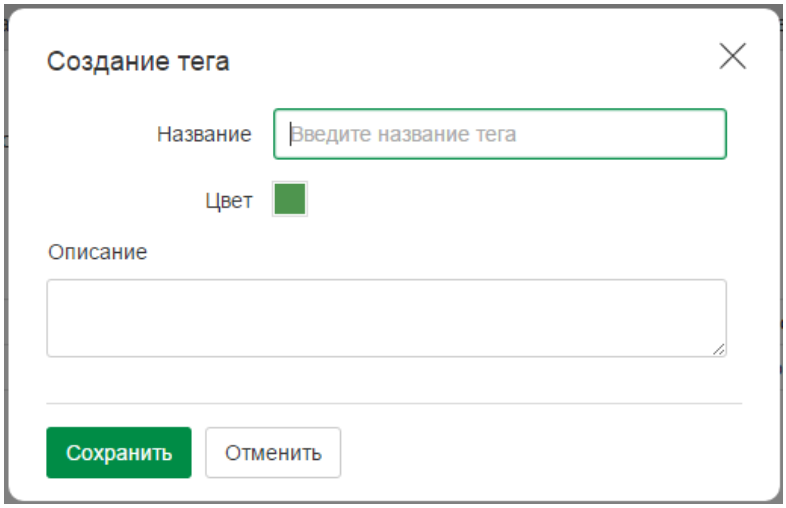
- "Раздел Списки" - о разделе, в котором ведется работа со списками

5.3.1 Работа с тегами

Цель:
Создать тег.

Решение:

1. Перейдите в раздел **Списки**, подраздел **Теги**.
2. На панели инструментов нажмите + **Создать тег**.



3. Укажите атрибуты добавляемого тега (см. "Теги").
4. Нажмите **Сохранить**.
5. При необходимости повторите добавление для наполнения справочника тегов.

Дополнительные сведения:
Редактирование и удаление тега выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.3.2 Работа со веб-ресурсами

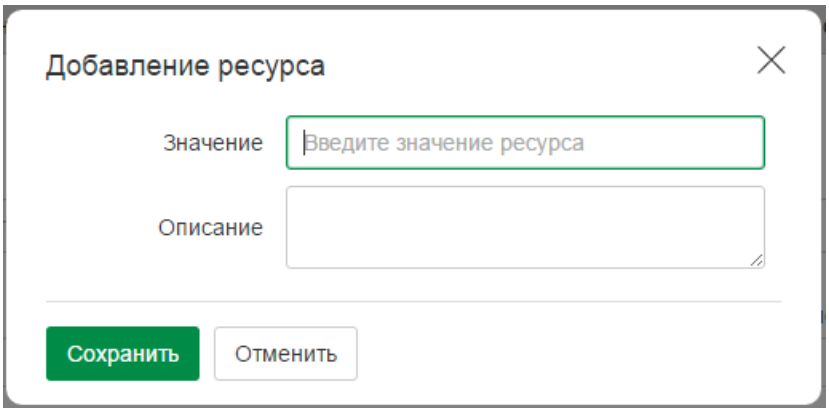
Цель:
Указать интернет-ресурсы, посещение которых будет детектироваться Системой как нецелевое использование рабочего времени. Для этого требуется:

1. Создать список ресурсов.
2. Добавить ресурсы в список.

Решение:

1. Создание группы ресурсов.
    a. Перейдите в раздел **Списки**, в подраздел **Ресурсы**.
    b. В левой части рабочей области нажмите + **Создание списка ресурсов**.
    c. В открывшемся окне введите название и описание списка ресурсов.
    d. Нажмите **Сохранить**.
2. Добавление ресурса.
    a. Перейдите в раздел **Списки**, в подраздел **Ресурсы**.
    b. В левой части рабочей области щелчком левой кнопки мыши выделите требуемый список ресурсов.

c. В правой части рабочей области на панели инструментов ресурсов нажмите + **Создать ресурс**.



d. В открывшемся окне **Добавление ресурса** введите атрибуты ресурса:
   - в поле **Значение** - наименование ресурса в сети Интернет;
   - в поле **Описание** - сопроводительный комментарий к записи о ресурсе (не обязательно).

e. Нажмите **Сохранить**.

Важно!

По завершении редактирования списка ресурсов требуется применить обновленную конфигурацию (см. "Применение конфигурации Системы").

Пример:

Если требуется, чтобы при посещении сотрудниками интернет-сайта EXAMPLE.COM Система помечала объект перехвата как *НЕЦЕЛЕВОЙ_САЙТ*:
Офицер безопасности создает группу ресурсов *НЕЦЕЛЕВОЙ_САЙТ*, а в созданной группе - ресурс *EXAMPLE.COM*.

Дополнительные сведения:

- Редактирование и удаление ресурсов и их групп ресурсов выполняются стандартным способом:
  - Редактирование элемента;
  - Удаление элемента.

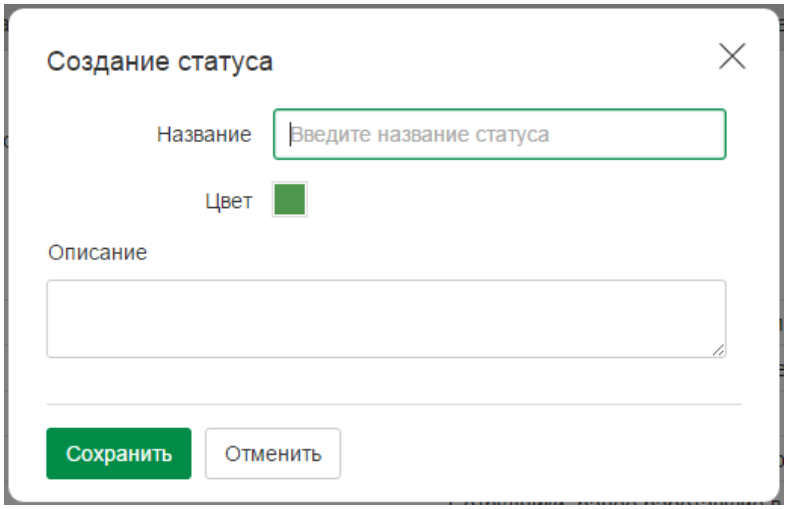
5.3.3 Работа со статусами

Цели:

1. Создать статус, характеризующий персону или рабочую станцию.
2. Создать политику контроля персон для персон, объединенных общим статусом.

Чтобы создать новый статус:

1. Перейдите в раздел **Списки**, в подраздел **Статусы**.
2. На панели инструментов нажмите **Создать статус**:



3. Укажите атрибуты добавляемого статуса (см. "Статусы").
4. Нажмите **Сохранить**.

Чтобы создать политику контроля персон непосредственно из подраздела Статусы:

1. Перейдите в раздел **Списки**, в подраздел **Статусы**.
2. В списке статусов выделите требуемый статус.
3. На панели инструментов нажмите **Создать политику**.
   Откроется раздел **Политики**, в котором будет отображаться новая политика контроля персон для персон с указанным статусом и форма ее просмотра (подробнее см. "Политики и форма их просмотра").

Дополнительные сведения:

Редактирование и удаление статуса выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.3.4 Работа с периметрами

Справочная информация:

Периметры позволяют логически разделить организацию на структурные элементы и отслеживать движение трафика.

По умолчанию в Системе создан периметр компании (название периметра может варьироваться). Для того чтобы к объектам перехвата применялись действия, указанные в предустановленных политиках, требуется добавить элементы в указанный периметр (см. Цель 2 в данной статье).

Примечание:

При создании периметра для выбора LDAP-домена в качестве элемента периметра необходимо предварительно настроить синхронизацию с LDAP-сервером и добавить домен через закладку **Группы**.

Цель:

1. Создать периметр.
2. Добавить элемент в периметр.

Решение:

1. Создание периметра.
    a. Перейдите в раздел **Списки**, в подраздел **Периметры**.
    b. В левой части рабочей области нажмите + **Создание периметра**.
    c. В открывшемся диалоговом окне в поле **Название** укажите название добавляемого периметра.
    d. В поле **Описание** введите описание периметра (необязательно).
    e. Нажмите **Сохранить**.
2. Добавление элемента в периметр.
    a. Перейдите в раздел **Списки**, в подраздел **Периметры**.
    b. В левой части рабочей области щелчком левой кнопки мыши выделите целевой периметр из списка периметров.
    c. В правой части рабочей области нажмите **Добавить элемент к периметру** и в раскрывающемся списке выберите требуемый тип элемента.
    d. В появившемся поле укажите один или несколько элементов одним из следующих способов:
        - Для *Персоны*, *Группы персон* или *Тематики ресурса*:
            - начните вводить название элемента в поле и выберите требуемую запись из раскрывшегося списка;
            - нажмите + **Добавить** справа от поля и в открывшемся диалоговом окне установите флажок в поле с целевым элементом. Нажмите **Добавить**.
        - Для *Адреса электронной почты*, *Web-ресурса*, *Телефона*, *Skype*, *ICQ*, *Домена* и *Lotus-контакта* - введите название (например, для *Web-ресурса*) или значение (например, для *IP-адреса*) в поле и нажмите **Enter** на клавиатуре.

> **Важно!**
>
> Для включения домена в периметр необходимо использовать его полное имя. Если указано доменное имя первого уровня, то домены вложенных уровней не будут включены в периметр. Например, при добавлении в периметр домена `domain.com`, домен вложенного уровня `basic.domain.com` не будет учитываться.

e. Введенные значения будут добавлены в список элементов. Чтобы удалить отдельный элемент из списка, нажмите X рядом с названием элемента. Чтобы удалить весь список элементов определенного типа, нажмите кнопку × напротив строки со списком элементов.



Пример:

1. Если требуется создать периметр *Бухгалтерия*:
   Офицер безопасности добавляет новый периметр и присваивает ему название *Бухгалтерия*.
2. Если требуется, чтобы в периметр *Бухгалтерия* входила группа *Финансисты* (включая все контактные данные всех персон, входящих в указанную группу), а также сотрудник Василий Сидоров (подразумевается, что *Василий Сидоров* уже создан в разделе **Персоны**), не входящий в группу *Финансисты*:
   Офицер безопасности выделяет периметр *Бухгалтерия* в списке периметров. Далее офицер безопасности:
   - добавляет группу *Финансисты*:
     - нажимает **Добавить элемент к периметру**;
     - в раскрывающемся списке выбирает **Группа персон**;
     - в поле **Группа персон** указывает *Финансисты*;
   - добавляет персону *Василий Сидоров*:
     - нажимает **Добавить элемент к периметру**;
     - в раскрывающемся списке выбирает **Персона**;
     - в поле **Персона** указывает *Василий Сидоров*.

Дополнительные сведения:

- Редактирование периметра выполняется стандартным способом (см. "Редактирование элемента").
- Удаление периметра выполняется стандартным способом (см. "Удаление элемента").

5.4 Работа с базой технологий

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Для чего требуется база технологий:
С помощью элементов базы технологий вы можете указать Системе, какая информация является конфиденциальной в рамках компании (т.е. разглашение какой информации является нарушением политики корпоративной безопасности). На основе базы технологий выполняется анализ действий персон, в результате которого выявляются нарушения политики корпоративной безопасности (например, отправка конфиденциального документа за пределы компании). *Базой технологий* называется набор элементов (терминов, текстовых объектов, эталонных документов и пр.), используемых для анализа перехваченных данных.

Помимо базы технологий, при анализе действий персон также используется список ресурсов, который позволяет выявить нецелевое использование рабочего времени (например, просмотр развлекательных Интернет-сайтов с рабочего компьютера). Подробнее об указании нецелевых ресурсов см. "Работа со списками ресурсов".

Настройка анализа действий персон состоит из следующих действий:

1. Определение конфиденциальной информации - создание базы технологий.
2. Указание нецелевых ресурсов - создание списка ресурсов, посещение которых на рабочем месте является нецелевым использованием рабочего времени.
3. Создание объектов защиты на основе элементов, входящих в базу технологий.

После этого вы можете создать политику и указать Системе, каким образом следует реагировать на обнаружение в перехваченных данных объектов защиты или отправке запросов на ресурсы, включенные в список нецелевых (см. "Настройка реакций Системы").

См. также:

- "Раздел Технологии" - о разделе, в котором ведется работа с базой технологий
- "Список ресурсов" - о подразделе, в котором ведется работа со списком ресурсов
- "Раздел Объекты защиты" - о разделе, в котором ведется работа с объектами защиты

5.4.1 Определение конфиденциальной информации

Цель:

Добавить в базу технологий элементы, на основе которых Система будет определять наличие конфиденциальных данных в объектах перехвата.

Решение:

1. Перейдите в какой-либо подраздел раздела **Технологии** (**Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати** или **Выгрузки из БД**).

Примечание.

Подраздел Графические объекты содержит только предустановленные элементы, для которых недоступны операции добавления, редактирования и удаления.

2. Создайте новую категорию в подразделе **Категории и термины** или новый каталог в других подразделах.
3. Наполните созданную категорию (или созданный каталог) примерами конфиденциальных данных, наличие которых в трафике будет указывать Системе на нарушение политики безопасности.
4. При необходимости повторите шаги 2 и 3.

Важно!

По завершении настройки базы технологий требуется применить обновленную конфигурацию (см. "Применение конфигурации Системы").

Подробнее о работе с элементами технологий:

Название технологии	Описание технологии	Действие
Категории и термины	Набор терминов и их категорий. Термин - слово или словосочетание, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста той категории, к которой относится найденный термин	Создание терминов и их категорий
Текстовые объекты	Текстовая информация, извлечённая из тела объекта и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска	Создание текстовых объектов
Эталонные документы	Документ, цитаты из которого ищутся в анализируемом тексте. Эталонными документами могут быть образцы текстов приказов, финансовых отчетов, договоров и других конфиденциальных документов. Эталонные документы хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы	Создание эталонных документов
Бланки	Бланк, версия которого ищется в сетевом трафике. Эталонными бланками могут служить различные анкеты, квитанции и проч. Эталонные бланки хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы	Создание эталонных бланков

Название технологии	Описание технологии	Действие
Печати	Изображение печати, которое ищется в сетевом трафике. Эталонными печатями могут быть изображения круглых оттисков, которые используются в организациях	Создание эталонных печатей
Выгрузки из баз данных	Часть базы данных, цитаты из которой ищутся в анализируемом тексте. Эталонными выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и прочее	Создание эталонных выгрузок из БД
Графические объекты	Изображение определенного типа, которое ищется в сетевом трафике. Графическими объектами могут быть изображения разворота паспорта или кредитной карты.	Все графические объекты в Системе являются предустановленными. Создание и редактирование графических объектов недоступно.

См. также:

- "Раздел Технологии" - о разделе, в котором ведется работа с базой технологий

5.4.1.1 Работа с категориями и терминами

Справочная информация:
Термины - набор данных, необходимых для проведения лингвистического анализа. Все термины сгруппированы по *категориям*.
Категории служат для классификации возможных нарушений политики безопасности. Наличие в тексте термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией.

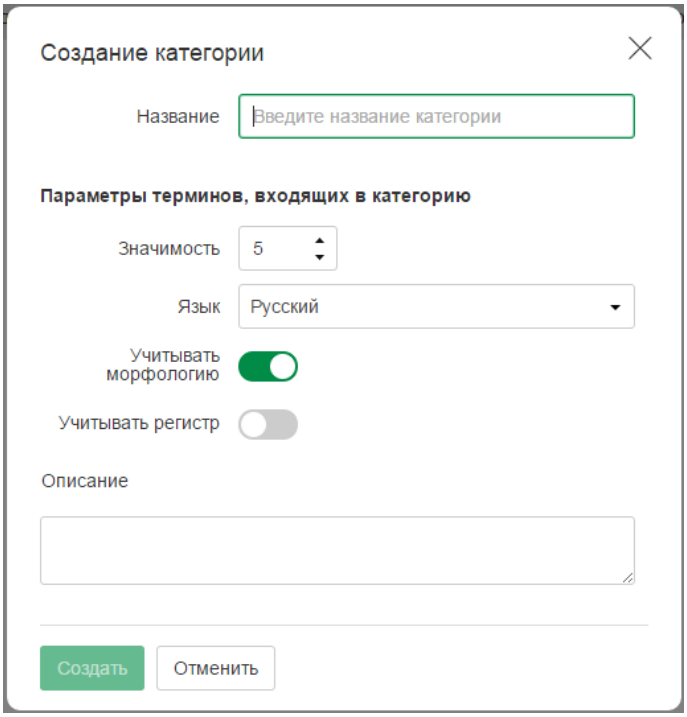
Цели:

1. Создать категорию терминов.
2. Создать термин внутри категории.

Решение:

5.4.1.1.1 1. Создание категории.

1.
   a. Перейдите в раздел **Технологии**->**Категории и термины**.
   b. В левой части рабочей области на панели инструментов нажмите + **Создать категорию**.



c. Укажите требуемые атрибуты для категории (см. "Категории").

d. Нажмите **Создать**.

5.4.1.1.2 2. Создание термина.

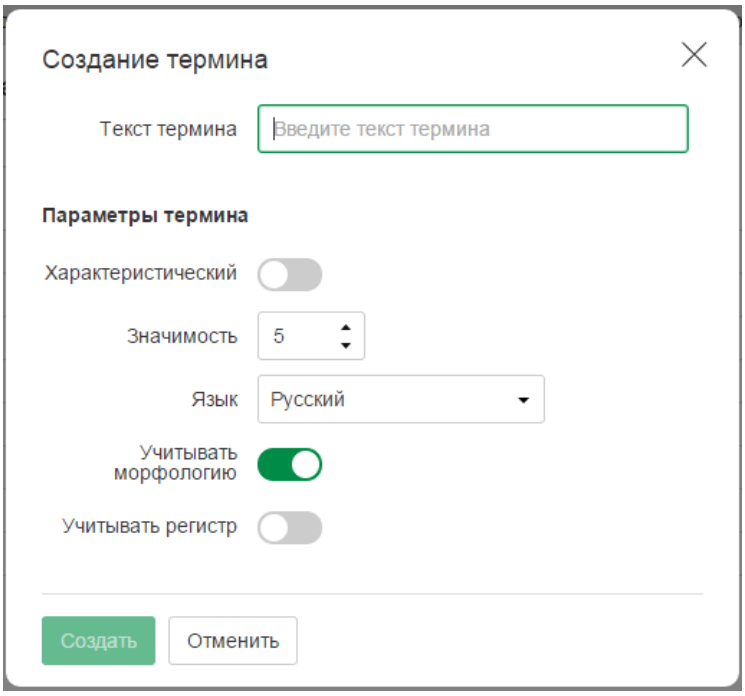
1.

a. Перейдите в раздел **Технологии**->**Категории и термины**.

b. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую категорию.

> **Примечание.**
>
> Для добавления терминов доступны только те категории, которые не включают других вложенных категорий.

c. На панели инструментов в правой части рабочей области нажмите + **Создать термин**.



d. Укажите требуемые атрибуты (см. "Термины").

e. Нажмите **Сохранить**.

Пример 1:
Если требуется, чтобы при наличии в трафике хотя бы одного словосочетания "Дата выдачи ИНН", Система помечала объект перехвата как *ДАТА_ВЫДАЧИ_ИНН*:

1. офицер безопасности выбирает целевую категорию,
2. добавляет в нее термин *Дата выдачи ИНН*,
3. включает настройку **Характеристический**.

При передаче данных, среди которых обнаруживается указанное словосочетание, Система присваивает объекту перехвата категорию *Дата выдачи ИНН*.

Пример 2:
Если требуется, чтобы при наличии в трафике фрагментов программного кода, Система помечала объект перехвата как утечку кода программы:
ОБ создает категорию *Утечка кода программы*, добавляет в нее термины *Procedure*, *Result*. В результате анализа переданных данных, среди которых обнаруживаются указанные термины, Система присваивает объекту перехвата категорию *Утечка кода программы*.

Важно!

Объекту перехвата присваивается только категория, непосредственно содержащая сработавший элемент (термин, эталонный документ и др.).
Например:
Категория А содержит категорию Б. Категория Б содержит термин В. Во время анализа события Система обнаружила в теле события наличие термина В.
В этом случае объекту перехвата будут проставлены термин В и категория Б.

Дополнительные сведения:

Редактирование и удаление терминов выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.4.1.2 Работа с текстовыми объектами

Цели:

1. Создать каталог текстовых объектов.
2. Создать текстовый объект и указать его значение.
3. Добавить системный текстовый объект в выбранный каталог.

Решение:

5.4.1.2.1 1. Создать каталог текстовых объектов.

1.

a. Перейдите в раздел **Технологии**->**Текстовые объекты**.

b. В левой части рабочей области на панели инструментов нажмите **Создать каталог текстовых объектов**.

c. В открывшемся окне введите название и описание каталога.

d. Нажмите **Сохранить**.

5.4.1.2.2 2. Создание текстового объекта и указание его значения.

1.

a. Перейдите в раздел **Технологии**->**Текстовые объекты**.

b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создан текстовый объект.

c. В правой части рабочей области на панели инструментов текстовых объектов нажмите **Создать текстовый объект**.

d. Введите название и описание текстового объекта.

e. Нажмите **Создать**. Новый текстовый объект будет добавлен в список.

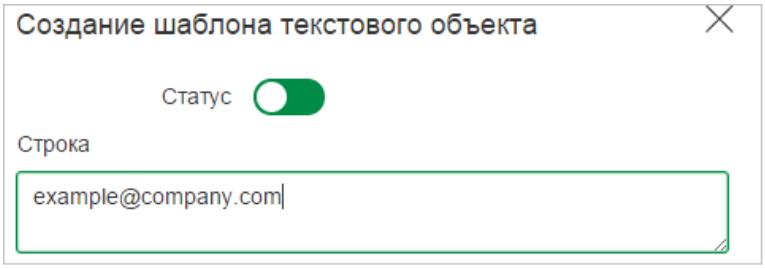
f. Выделите текстовый объект в списке и нажмите **Редактировать**.

g. Создайте шаблон для текстового объекта и укажите его параметры (см. "Шаблоны текстовых объектов").

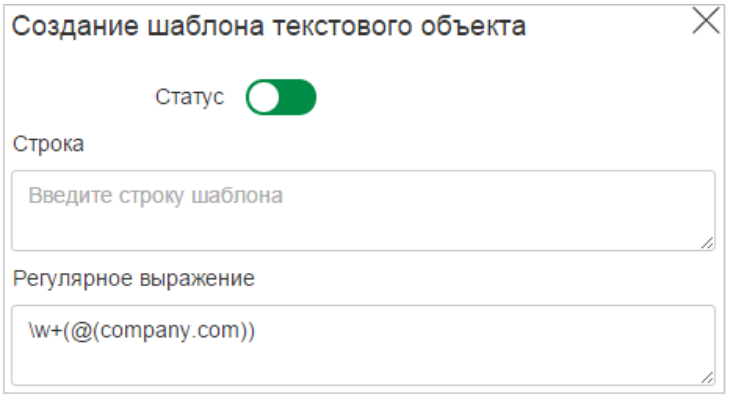
h. Нажмите **Сохранить**.

Пример:
1) Если требуется, чтобы Система определяла наличие в трафике адреса электронной почты "example@company.com" и определяла его как текстовый объект EXAMPLE_MAIL:
Офицер безопасности создает активный текстовый объект *EXAMPLE_MAIL*. Затем Офицер безопасности выделяет новый созданный текстовый объект щелчком левой кнопки мыши,

переходит в режим редактирования объекта и создает для него новый активный шаблон, указав в качестве значения строку `example@company.com`:



2) Если требуется, чтобы Система определяла наличие в трафике адреса электронной почты с доменом "company.com" и определяла его как текстовый объект *COMPANY_MAIL*:
Офицер безопасности создает активный текстовый объект *COMPANY_MAIL*. Затем Офицер безопасности выделяет новый созданный текстовый объект щелчком левой кнопки мыши, переходит в режим редактирования объекта и создает для него новый активный шаблон, указав в качестве значения регулярное выражение: `\w+(@(company.com))`



Примечание:

В Системе используется стандартный язык регулярных выражений. Подробную информацию о регулярных выражениях Вы можете найти, например, в интернет-статье "Регулярные выражения, пособие для новичков".

3. Добавление системного текстового объекта в каталог.

1.

a. Перейдите в раздел **Технологии**->**Текстовые объекты**. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую категорию.

b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, в который требуется добавить текстовый объект.

c. В правой части рабочей области на панели инструментов текстовых объектов нажмите ▾ и в раскрывающемся списке выберите **Добавить системный текстовый объект**.

d. В открывшемся окне поставьте галочку напротив текстовых объектов, которые Вы хотите добавить.

> **Примечание:**
>
> Для поиска требуемых текстовых объектов в списке введите искомый текст в строку **Поиск**.

e. Нажмите **Добавить**.

> **Примечание:**
>
> Системные текстовые объекты уже содержат предустановленные шаблоны. Однако Вы также можете добавить пользовательский шаблон для выбранного системного объекта. Для этого выполните шаги **f**-**h** из пункта **2.Создание текстового объекта и указание его значения**.

Дополнительные сведения:
Редактирование и удаление текстовых объектов, их значений и каталогов выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.4.1.3 Работа с эталонными документами

Цели:

1. Создать каталог эталонных документов.
2. Создать эталонный документ внутри каталога.
3. Обновить эталонный документ.

Решение:

1. Создать каталог эталонных документов

1.

a. Перейдите в раздел **Технологии**->**Эталонные документы**.

b. В левой части рабочей области на панели инструментов нажмите **Создать каталог эталонных документов**.

c. В открывшемся окне укажите параметры нового каталога (см. "Эталонные документы").

d. Нажмите **Создать**.

2. Создать эталонный документ

1.

a. Перейдите в раздел **Технологии**->**Эталонные документы**.

b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создан эталонный документ.

c. В правой части рабочей области на панели инструментов эталонных документов нажмите + **Добавить**.

d. В открывшемся диалоговом окне выберите тип данных, которые могут содержаться в документе: **Текстовые** или **Все типы** (могут содержать текст, изображения и бинарные данные).

e. Нажмите **Выбрать файлы** и в открывшемся окне укажите документ, с которого требуется снять цифровой отпечаток. Нажмите **Открыть**.
Выберите для загрузки текстовый файл, изображение или архив в соответствии с типом данных, указанным на шаге d. При этом действуют следующие правила:

- Если формат выбранного файла не поддерживается Системой, то цифровой отпечаток будет загружен как бинарные данные.
- Если для загрузки выбран архив, то в качестве эталонных документов будут добавлены содержащиеся в архиве файлы.

f. После окончания загрузки эталонный документ будет добавлен в каталог. Все обязательные атрибуты присваиваются созданному эталонному документу по умолчанию.

Примечание:

Если Системе не удалось загрузить файл эталонного документа, в окне загрузки будет выведено сообщение об ошибке.

Важно!

Требования к размеру файла:

- Максимальный размер бинарных данных - 128 Мбайт;
- Максимальный размер текстовых данных - 30 Мбайт;
- Минимальный размер бинарных или текстовых данных – 128 байт;
- Минимальный размер plain text для текстовых данных - 10 символов;
- Минимальный размер изображения - 100 пикселей по одной стороне;
- Допустимое соотношение сторон - не больше 5:1.

g. Для изменения указанных Системой атрибутов эталонного документа на панели инструментов нажмите **Редактировать** и измените требуемые параметры (см. "Эталонные документы").

3. Обновить эталонный документ

1.

a. Перейдите в раздел **Технологии**->**Эталонные документы**.

b. В левой части рабочей области выберите требуемый каталог.

c. В правой части рабочей области выделите в списке эталонный документ, который требуется обновить.

d. Нажмите **Редактировать**.

e. В открывшемся окне редактирования документа нажмите **Обновить**.

f. Нажмите **Выбрать файл**.

g. В открывшемся диалоговом окне укажите документ, который будет использоваться для обновления, и нажмите **Открыть**.

h. Начнется загрузка файла. После окончания загрузки эталонный документ будет дополнен новыми данными в соответствии с выбранным режимом обновления. Если Системе не удалось выполнить обновление, в окне загрузки будет выведено сообщение об ошибке.

Примечание.

При обновлении эталонного документа Система заменяет данные обновляемого документа на данные из файла обновления.

Пример:
Если требуется, чтобы при наличии в трафике хотя бы 30% текста документа "Внутренний регламент компании", Система помечала объект перехвата как *ВНУТРЕННИЙ_РЕГЛАМЕНТ_КОМПАНИИ*:

1.

a. Офицер безопасности переходит в требуемый каталог,

b. загружает файл документа "Внутренний регламент компании" в качестве эталонного документа,

c. указывает атрибуту **Название** значение *ВНУТРЕННИЙ_РЕГЛАМЕНТ_КОМПАНИИ*

d. указывает атрибуту **Порог цитируемости текстовых данных** значение **30**.

Если требуется, чтобы при наличии в трафике хотя бы 10% бинарного содержимого исполнимого файла "`Setup.exe`", Система помечала объект перехвата как *SETUP_EXE*:

1.

a. Офицер безопасности переходит в требуемую категорию,

b. загружает файл "`Setup.exe`" в качестве эталонного документа,

c. указывает атрибуту **Название** значение *SETUP_EXE,*

d. указывает атрибуту **Порог цитируемости бинарных данных** значение **10**.

Дополнительные сведения:
Редактирование и удаление эталонных документов и их каталогов выполняется стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.4.1.4 Работа с бланками

Цель:

1. Создать каталог эталонных бланков.
2. Создать эталонный бланк.
3. Обновить эталонный бланк.

Решение:

1. Создать каталог эталонных бланков

1.

a. Перейдите в раздел **Технологии**->**Бланки**.

b. В левой части рабочей области на панели инструментов нажмите **Создать каталог эталонных бланков**.

c. В открывшемся окне введите название и описание каталога.

d. Нажмите **Создать**.

2. Создать эталонный бланк

1.

a. Перейдите в раздел **Технологии**->**Бланки**.

b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создана эталонный бланк.

c. В правой части рабочей области на панели инструментов форм нажмите **Добавить**.

d. В открывшемся диалоговом окне укажите документ, который будет служить примером эталонного бланка, и нажмите **Открыть**. Вы можете загрузить документ в одном из следующих форматов: DOC, DOCX, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF, CHM.

e. После окончания загрузки эталонный бланк будет добавлен в каталог. Все обязательные атрибуты присваиваются созданному эталонному бланку по умолчанию.

> **Примечание:**
>
> Если Системе не удалось загрузить файл эталонного бланка, в окне загрузки будет выведено сообщение об ошибке.

f. Для изменения атрибутов эталонного бланка, заданных в Системе по умолчанию, на панели инструментов нажмите **Редактировать** и измените требуемые атрибуты (см. "Бланки").

3. Обновить эталонный бланк

1.

a. Перейдите в раздел **Технологии**->**Бланки**.

b. В левой части рабочей области выберите требуемый каталог.

c. В правой части рабочей области выделите в списке бланк, который требуется обновить.

d. Нажмите



Редактировать.

e. В открывшемся окне редактирования бланка нажмите **Обновить**.

f. Нажмите **Выбрать файл**.

g. В открывшемся диалоговом окне укажите файл, который будет использоваться для обновления, и нажмите **Открыть**. Начнется загрузка.

h. Данные эталонного бланка будут заменены данными из файла обновления.
Если Системе не удалось выполнить обновление, в окне загрузки будет выведено сообщение об ошибке.

Пример:

Если требуется, чтобы при наличии в трафике фрагментов даже незаполненной анкеты "Анкета соискателя" Система помечала объект перехвата как *АНКЕТА_СОИСКАТЕЛЯ*:

1. Офицер безопасности создает бланк *АНКЕТА_СОИСКАТЕЛЯ*,
2. загружает файл документа "Анкета соискателя" в качестве эталонного бланка,
3. создает новый объект защиты на основе бланка *АНКЕТА_СОИСКАТЕЛЯ*,
4. в условиях обнаружения эталонного бланка устанавливает флажок в поле **Заполненные и незаполненные**.

Дополнительные сведения:
Редактирование и удаление бланков и их каталогов выполняется стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.4.1.5 Работа с печатями

Цели:

1. Создать каталог эталонных печатей.
2. Создать эталонную печать.

Решение:

1. Создать каталог эталонных печатей

1.

a. Перейдите в раздел **Технологии**->**Печати**.

b. В левой части рабочей области на панели инструментов нажмите



Создать каталог эталонных печатей.

c. В открывшемся окне укажите параметры нового каталога.

d. Нажмите **Создать**.

2. Создать эталонную печать

1.

a. Перейдите в раздел **Технологии**->**Печати**.

b. В левой части рабочей области рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создана эталонная печать.

c. В правой части рабочей области на панели инструментов печатей нажмите  **Добавить**.

d. В открывшемся диалоговом окне укажите документ, который будет служить примером эталонной печати, и нажмите **Открыть**.

e. После окончания загрузки эталонная печать будет добавлена в каталог. Все обязательные атрибуты присваиваются созданной эталонной печати по умолчанию.

> **Примечание:**
>
> Если Системе не удалось загрузить файл эталонной печати, в окне загрузки будет выведено сообщение об ошибке.

f. Для изменения указанных Системой атрибутов эталонной печати на панели инструментов нажмите  **Редактировать** и измените требуемые атрибуты (см. "Печати").

> **Примечание:**
>
> Создание эталонной печати подробнее описано в статье Базы знаний InfoWatch "Использование детектора эталонных печатей".

Пример:
Если требуется, чтобы при наличии в трафике изображения печати организации Система помечала объект перехвата как *КРУГЛАЯ_ПЕЧАТЬ*:

1.

a. Офицер безопасности подготавливает файл "`Stamp.png`", в котором на квадратном холсте с белым фоном во весь размер холста размещено изображение печати организации,

b. переходит в требуемый каталог печатей,

c. загружает файл с изображением печати "Stamp.png" в качестве эталонной печати,

d. создает объект защиты *КРУГЛАЯ_ПЕЧАТЬ* на основе созданной эталонной печати.

Дополнительные сведения:
Редактирование и удаление печатей и их каталогов выполняется стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.4.1.6 Работа с выгрузками

Цель:

1. Создать каталог эталонных выгрузок.
2. Создать эталонную выгрузку из БД.
3. Обновить эталонную выгрузку.

Решение:

1. Создать каталог эталонных выгрузок

1.
   a. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
   b. В левой части рабочей области на панели инструментов нажмите
   
   Создать каталог выгрузок из БД.
   c. В открывшемся окне введите название и описание каталога.
   d. Нажмите **Создать**.

2. Создать эталонную выгрузку

1.
   a. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
   b. В левой части рабочей области выделите группу, в которую требуется добавить выгрузку.
   c. В правой части рабочей области на панели инструментов нажмите  **Добавить**.
   d. В открывшемся диалоговом окне укажите требуемый файл для загрузки в формате CSV или TSV и нажмите **Открыть**.

> **Важно!**
>
> При использовании Postgre SQL размер эталонной выгрузки не должен превышать 1Гб.

   e. После успешной загрузки файла:
      - нажмите **Настроить выгрузку из БД** - для настройки эталонной выгрузки;
      - закройте окно **Создание выгрузки из базы данных** - для выхода без дополнительных настроек.
   f. Укажите требуемые атрибуты (см. "Выгрузки из БД" и "Условия детектирования выгрузки").
   g. Нажмите **Сохранить**.

3. Обновить эталонную выгрузку

1. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
2. В левой части рабочей области выберите требуемый каталог.
3. В правой части рабочей области выделите в списке эталонную выгрузку, которую требуется обновить.

4. Нажмите  **Редактировать**.
5. В открывшемся окне редактирования выгрузки нажмите **Обновить**.
6. Укажите требуемый режим обновления: **Добавление новых записей** или **Удаление старых записей и добавление новых**.
7. Нажмите **Выбрать файл**.
8. В открывшемся диалоговом окне укажите файл, который будет использоваться для обновления, и нажмите **Открыть**. Начнется загрузка.
9. После окончания загрузки эталонная выгрузка из БД будет дополнена новыми данными в соответствии с выбранным режимом обновления. Если Системе не удалось выполнить обновление, в окне загрузки будет выведено сообщение об ошибке.

Дополнительные сведения:
Редактирование и удаление эталонных выгрузок из БД и их каталогов выполняются стандартным способом:

-
  - Редактирование элемента;
  - Удаление элемента.

5.4.1.6.1 Условия детектирования выгрузки

Справочная информация:

Выполнение условий детектирования позволяет соотнести объект перехвата с определенной эталонной выгрузкой.

Вы можете указать несколько (не более 20) условий детектирования для эталонной выгрузки. В этом случае для отнесения объекта перехвата к данной выгрузке достаточно выполнения хотя бы одного из условий.

Цель:

Добавить условие детектирования выгрузки.

Решение:

1. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
2. В левой части рабочей области выберите требуемый каталог.
3. В правой части рабочей области выделите в списке требуемую эталонную выгрузку и нажмите  **Редактировать**.
   Откроется форма редактирования выгрузки.
4. На панели инструментов, расположенной под заголовком **Условия детектирования выгрузки**, нажмите  **Добавить**.
5. В открывшемся диалоговом окне укажите следующие параметры (подробное описание параметров смотрите ниже):
   a. **Название условия**;
   b. **Минимальное количество строк**;

c. **Правило детектирования**.

6. Нажмите **Создать**.

Параметры условия детектирования заполняются в соответствии со следующими рекомендациями:

Правило детектирования.

Правило детектирование содержит номера столбцов и логические отношения между ними. Если при анализе в объекте перехвата обнаружены данные из указанных ячеек с учетом заданных отношений, то данная строка считается сработавшей.

Примечание:

Для исключения ложноположительных срабатываний в Системе используются стоп-слова: цифры, буквы и слова, нахождение которых в ячейках не приводит к срабатыванию этих ячеек. Полный список стоп-слов см. в статье Базы знаний InfoWatch " Список стоп-слов для эталонных выгрузок из баз данных ".

Список **Доступные столбцы в выборке** содержит столбцы, которые могут быть использованы для создания условия. Поле **Поиск** позволяет найти нужный столбец по его названию.

Логические отношения задаются с помощью символов:

1. "+" - конъюнкция ячеек (логическое "И");
2. "|" - дизъюнкция ячеек (логическое "ИЛИ");

Примечание.

Условие вида (1|3) должно указываться в скобках.

3. "()" - группировка условий. Например, условие вида 1+(2|3) означает, что строка считается сработавшей, если в ней сработала первая ячейка, а также вторая или третья ячейка.

   Условие вида (1|3)+(5|4) означает, что строка считается сработавшей, если сработала первая или третья ячейка и пятая или четвёртая ячейка.

Важно!

Символ "|" не может использоваться для разделения групп в скобках. То есть условие (1+8+11*)|(2+3*) должно быть представлено в виде двух отдельных условий: 1+8+11* и 2+3*.

4. "*" - символ астериска позволяет учитывать также незаполненные ячейки. Например, условие вида 1+2* означает, что строка считается сработавшей, если в ней сработала первая и вторая ячейка, при этом вторая ячейка может быть незаполненной.

Важно!

Технология анализа не учитывает спецсимволы, поэтому, если столбец содержит адрес электронный почты, для уменьшения ложных срабатываний рекомендуется указать дополнительный столбец (например, ФИО).

Минимальное количество строк.

Минимальное количество строк, которое требуется обнаружить для срабатывания правила.

Например, если указано условие вида: 1+(2|3) и задано минимальное количество строк = 10, то для срабатывания условия необходимо, чтобы в анализируемом тексте содержалось не менее 10 различных строк, удовлетворяющих условию 1+(2|3).

Пример:
Если требуется, чтобы Система помечала объект перехвата как НОМЕРА_ТЕЛЕФОНОВ при обнаружении в нем не менее 7 строк с заполненными столбцами 1 и 4 из таблицы со следующей структурой:

Фамилия	Имя	Отчество	Номер телефона
Иванов	Иван	Иванович	89441234347
Петров	Петр	Петрович	83531355424
Сидоров	Сидор	Сидорович	83544593406
Смирнов	Юрий	Борисович	83245446441
Кузнецов	Владимир	Андреевич	84534359243
Соколов	Михаил	Григорьевич	83544352925

1. Офицер безопасности сохраняет таблицу в формате CSV или TSV и загружает созданный файл в Систему;
2. выполняет настройку правила обработки столбцов таблицы:
    - в поле **Правило детектирования** указывает **1+4**;
    - в поле **Минимальное количество строк** указывает **7**.
3. создает объект защиты "НОМЕРА_ТЕЛЕФОНОВ" на основе созданной выгрузки из БД.

При передаче трафика, в котором обнаруживаются указанные колонки данных, в Системе срабатывает объект защиты *НОМЕРА_ТЕЛЕФОНОВ*.

Дополнительные сведения:
Редактирование и удаление условий детектирования выгрузки выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

5.4.2 Экспорт и импорт базы технологий

Цель:

- сохранить XML-документ, содержащий базу технологий, на жесткий диск компьютера;
- загрузить базу технологий, хранящуюся на компьютере в виде XML-документа, для использования в Консоли управления InfoWatch Traffic Monitor.

Примечание:

Экспорт и импорт технологий не могут быть выполнены, если конфигурация Системы находится на редактировании. В этом случае будет выведено сообщение об ошибке.

Чтобы экспортировать базу технологий:

1. Перейдите в какой-либо подраздел раздела **Технологии** (**Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати** или **Выгрузки из БД**).
2. На панели инструментов в левой части рабочей области нажмите и в раскрывающемся списке выберите **Экспортировать**.
3. В открывшемся диалоговом окне **Сохранить как** укажите место на диске, куда будет сохранен xml-файл.
4. Нажмите **Сохранить**. Xml-файл будет сохранен на Ваш компьютер. Данный файл содержит следующие элементы:
   - категории и термины;
   - текстовые объекты, в том числе предустановленные;
   - эталонные документы;
   - бланки;
   - печати;
   - выгрузки из БД;
   - графические объекты.

   Структура каталогов при экспорте сохраняется.

Важно!

Экспортируется база технологий из последней примененной конфигурации (см. "Работа с конфигурацией Системы").

Чтобы импортировать базу технологий, хранящуюся на компьютере в виде XML-документа:

1. Перейдите в какой-либо подраздел раздела **Технологии** (**Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати** или **Выгрузки из БД**).

2. На панели инструментов в левой части рабочей области нажмите ▾ и в раскрывающемся списке выберите **Импортировать** .
3. В открывшемся диалоговом окне **Открыть** укажите xml-файл, который Вы хотите загрузить.
4. Нажмите **Открыть** и дождитесь окончание загрузки данных в Систему.

> **Примечание:**
>
> Если название каталога в файле импорта совпадает с названием каталога в Системе, но различаются пути к каталогу, то каталог из файла импорта добавлен не будет. Если название каталога в файле импорта совпадает с названием каталога в Системе, и путь к каталогу также совпадает, то данные из файла импорта будут объединены с данными, содержащимися в Системе.

Особенности слияния данных при импорте:

1. Для каталогов будут добавлены следующие элементы, отсутствующие в Системе:
   а) дочерние каталоги;
   б) элементы технологий.
2. Для категории будут добавлены термины, отсутствующие в Системе.
3. Для текстового объекта будут добавлены шаблоны, отсутствующие в Системе.

> **Примечание:**
>
> Имеющиеся в Системе верифицирующие функции будут заменены функциями из файла.

4. Для выгрузки из БД будут добавлены представления эталонной выгрузки, если содержимое выгрузки в файле и в Системе не отличается.

5.5 Работа с объектами защиты

Для чего требуются объекты защиты:

Использование объектов защиты позволяет анализировать перехваченные данные на предмет наличия в них сразу нескольких элементов анализа: например, эталонного документа, текстового объекта и выгрузки из базы данных. Таким образом вы можете настроить Систему на детектирование определенных бизнес-документов: например, паспорта транспортного средства или заявления о страховой выплате.

Работа с объектами защиты состоит из следующих действий:

Действие	Описание
Создание каталога объектов защиты	Создание каталога, в который будут добавлены объекты защиты
Создание объекта защиты	Создание объекта защиты и указание его параметров
Добавление элементов анализа	Добавление в объект защиты элементов анализа
Добавление условий обнаружения	Указание условий обнаружения для добавленных элементов анализа
Создание политики для объектов защиты и их каталогов	Создание политики защиты данных для выбранных объектов защиты и их каталогов
Импорт и экспорт объектов защиты	Импорт и экспорт структуры каталогов, содержащихся в них объектов и используемых элементов анализа
Активация и деактивация объектов защиты	Изменение статуса объектов защиты и их каталогов

См. также:

- "Раздел Объекты защиты" - о разделе, в котором ведется работа с объектами защиты

5.5.1 Создание каталога объектов защиты

Цель:
Создать каталог, в котором будут содержаться объекты защиты.

Решение:

1. Перейдите в раздел **Объекты защиты**.
2. На панели инструментов в левой части рабочей области нажмите **Создать каталог объектов защиты**.

> **Примечание:**
>
> Вы можете создать новый каталог объектов защиты внутри имеющегося каталога. Для этого выберите целевой каталог в списке.

3. В открывшемся диалоговом окне укажите атрибуты каталога.
4. Нажмите **Создать**.

Вы можете переместить выбранный каталог, используя перетаскивание. Для этого выделите каталог в списке и, удерживая левую клавишу мыши зажатой, переместите его в требуемое место в структуре каталогов, после чего отпустите зажатую клавишу мыши.

> **Примечание:**
>
> Перемещение каталога выполняется со всеми вложенными элементами: подкаталогами и

объектами защиты. При перемещении каталога его статус меняется на статус каталога, в который выполняется перемещение.

Дополнительные сведения:

Редактирование и удаление каталога объектов защиты выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.5.2 Создание объекта защиты

Цель:
Создать объект защиты на основе имеющихся в Системе элементов анализа.

Решение:

1. Перейдите в раздел **Объекты защиты**.
2. В левой части рабочей области выберите каталог, в который требуется добавить новый объект защиты, либо создайте новый каталог (см. "Создание каталогов объектов защиты").
3. На панели инструментов в правой части рабочей области нажмите + **Создать объект защиты**.
4. В открывшемся окне отметьте элементы, на основе которых будет создан объект защиты (см. "Добавление элементов анализа").
5. Определите, должны ли выбранные элементы анализа входить в один объект защиты, либо для каждого элемента будет создан отдельный объект:
   - Если выбрана настройка **Создать объект защиты на каждый выбранный элемент**, будет создан набор объектов защиты для каждого выбранного элемента анализа. Атрибуты созданных объектов защиты будут сформированы автоматически. Названия объектов будут сформированы из технологии элемента и названия элемента, например: "*Текстовый объект: Номер кредитной карты*".
   - Если настройка **Создать объект защиты на каждый выбранный элемент** не выбрана, то после нажатия **Создать** будет открыто дополнительное окно настроек параметров объекта защиты: см. шаг 7.
6. Нажмите **Создать**.
7. Если на шаге 5 настройка **Создать объект защиты на каждый выбранный элемент** не была выбрана, откроется окно **Создание объекта защиты**. В этом окне:
   a. Введите название объекта защиты.
   b. На вкладке **Элементы анализа**, содержащей выбранные элементы (см. "Элементы анализа"), вы можете добавить дополнительные элементы (для этого нажмите **Выбрать элементы**), а также удалить элементы из списка (нажмите на крестик в строке выбранного элемента).
   c. На вкладке **Условия обнаружения** укажите условия, при выполнении которых объекты защиты будут детектироваться в перехваченных данных (подробнее см. "Добавление условий обнаружения").

d. При необходимости, введите произвольный текст в поле **Описание**.

e. Нажмите **Создать**.

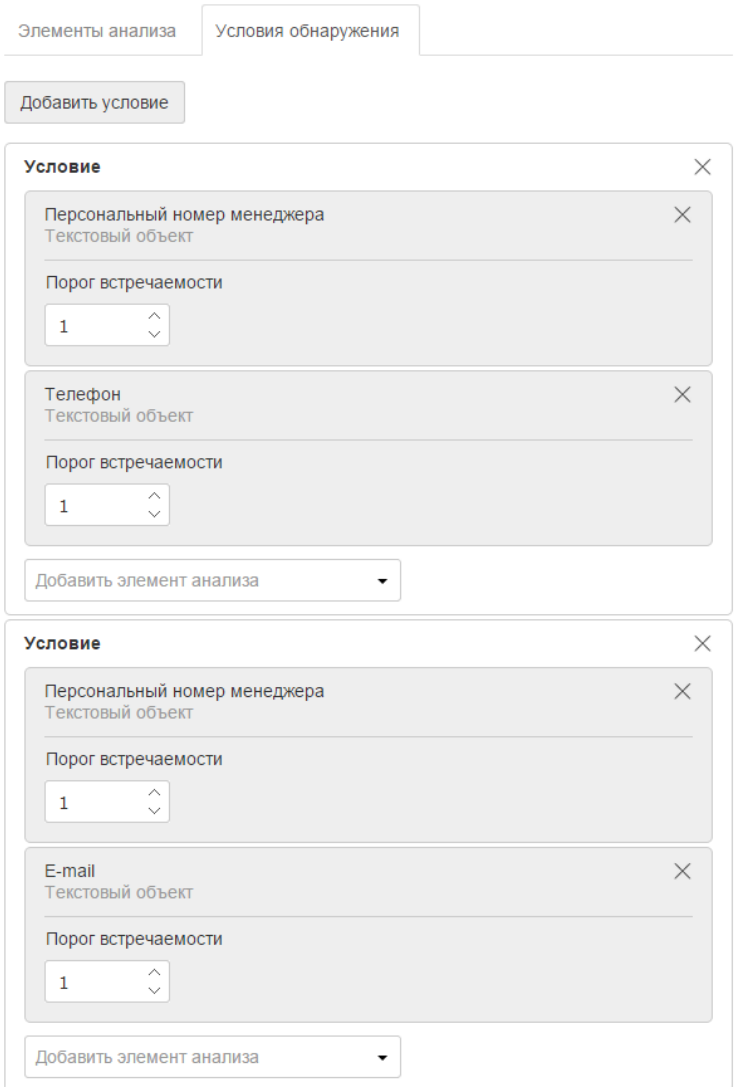
В результате в выбранном каталоге будет создан объект защиты (или несколько, если выбрана настройка **Создать объект защиты на каждый выбранный элемент**).Вы можете переместить созданный объект защиты в какой-либо другой каталог. Для этого выделите требуемый объект защиты и, удерживая левую клавишу мыши зажатой, переместите его в другой каталог, после чего отпустите зажатую клавишу мыши.
Пример: Требуется создать объект защиты *"Персональные данные менеджера"*, который должен детектироваться в Системе при выполнении одного из следующих условий:

- объект перехвата содержит персональный номер менеджера и E-mail;
- объект перехвата содержит персональный номер менеджера и номер телефона.

В этом случае офицер безопасности создает новый объект защиты, добавляет в него элементы анализа:

- текстовый объект *"Персональный номер менеджера"*;
- текстовый объект *"E-mail"*;
- текстовый объект *"Телефон"*;

и указывает следующие условия обнаружения для выбранных элементов анализа:



Дополнительные сведения:

Редактирование и удаление объектов защиты выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.5.3 Добавление элементов анализа

Цель:
Добавить элементы анализа в объект защиты.

Решение:

1. Перейдите в режим создания или редактирования объекта защиты (подробнее см. "Создание объекта защиты"). Если Вы находитесь в режиме редактирования объекта защиты, нажмите на кнопку **Выбрать элементы**.
2. В открывшемся окне добавления элементов анализа перейдите на нужную вкладку.

3. В списке элементов анализа отметьте элементы, которые вы хотите добавить.

> **Примечание.**
>
> При выборе категории, содержащей подкатегории (вкладка **Категория**), будут выбраны все подкатегории. Если требуется добавить отдельные подкатегории, нажмите на стрелочку слева от названия категории и в раскрывшемся списке установите флажки в нужных полях.

4. Нажмите **Создать**, если вы находитесь в режиме создания объекта защиты, или **Добавить**, если Вы находитесь в режиме редактирования.

> **Примечание.**
>
> Если выбрана настройка **Создать объект защиты на каждый выбранный элемент**, то для каждого элемента анализа будет создан отдельный объект защиты. Атрибуты объектов защиты будут заданы Системой по умолчанию.

Для удаления элемента анализа нажмите на крестик напротив требуемого элемента.

5.5.4 Добавление условий обнаружения

Справочная информация:

Объект защиты будет обнаружен в событии, если:

1. Объект защиты имеет статус - **Активный**.
2. В событии найдены элементы анализа, входящие в объект защиты, с учетом указанных условий обнаружения.

Каталог объектов защиты будет обнаружен в событии, если:

1. Каталог объектов защиты имеет статус - **Активный**.
2. В событии найден хотя бы один объект защиты, входящий в данный каталог.

Цель:

Добавить условия обнаружения для объекта защиты.

Решение:

1. Перейдите в режим редактирования объекта защиты, на вкладку **Условия обнаружения**.

> **Примечание.**
>
> Условия обнаружения можно указать также при создании объекта защиты (см. "Создание объекта защиты", шаг 7c).

2. В поле **Добавить элемент анализа** нажмите на стрелочку ▾ и в раскрывающемся списке выберите требуемый элемент.

Выбранный элемент будет добавлен в список условий. Для некоторых элементов анализа вы также можете указать дополнительные условия обнаружения (см. "Условия обнаружения").

3. Если объект защиты содержит несколько элементов анализа, добавьте условия обнаружения для остальных элементов одним из следующих способов:
    - Если требуется, чтобы условия были объединены с помощью операции конъюнкции (логическое "И"), добавьте условие, как описано на шаге 2.
      В этом случае все добавленные условия будут помещены в один блок **Условие** и объединены между собой с помощью операции конъюнкции.
    - Если требуется, чтобы условия (или группы условий) были объединены с помощью операции дизъюнкции (логическое "ИЛИ"), нажмите кнопку **Добавить условие**.
      Будет добавлен новый блок **Условие**, внутри которого вы можете добавить условия, как описано на шаге 2.
      В этом случае все блоки **Условие** будут объединены между собой с помощью операции дизъюнкции, а условия внутри одного блока - с помощью операции конъюнкции.
4. Нажмите **Сохранить**, если вы находитесь в режиме редактирования, или **Создать**, если вы находитесь в режиме создания объекта защиты.

Дополнительные сведения:

Удаление условий выполняется следующим способом:

- для удаления условия нажмите на крестик в правом верхнем углу панели с требуемых условием;
- для удаления блока, содержащего условия, нажмите на крестик в правом верхнем углу блока.

5.5.5 Создание политики для объектов защиты и их каталогов

Цель:

Создать политику защиты данных, настроенную на обнаружение объектов защиты, непосредственно из раздела "Объекты защиты".

Чтобы создать политику для каталога объектов защиты:

1. Перейдите в раздел **Объекты защиты**.
2. В списке **Каталоги объектов защиты** в левой части рабочей области выберите требуемый каталог.
3. На панели инструментов в левой части рабочей области нажмите на кнопку и в раскрывающемся списке выберите пункт **Создать политику**.
4. В открывшемся окне создания политики защиты данных укажите требуемые параметры (подробнее см. "Политики и форма их просмотра").
5. Нажмите **Сохранить**.

Созданная политика защиты данных будет срабатывать при обнаружении хотя бы одного объекта защиты, входящего в выбранный каталог.

Чтобы создать политику для выбранных объектов защиты:

1. Перейдите в раздел **Объекты защиты**.
2. В списке **Каталоги объектов защиты** в левой части рабочей области выберите требуемый каталог.
3. В правой части рабочей области отобразится список объектов защиты, входящих в выбранный каталог. Выделите требуемый объект защиты с помощью мыши. Чтобы выделить несколько объектов, используйте клавиши Shift или Ctrl.
4. На панели инструментов в правой части рабочей области нажмите на кнопку и в раскрывающемся списке выберите пункт **Создать политику**.
5. В открывшемся окне создания политики защиты данных укажите требуемые параметры (подробнее см. "Политики и форма их просмотра").
6. Нажмите **Сохранить**.

Созданная политика защиты данных будет срабатывать при обнаружении хотя бы одного из выбранных объектов защиты.

5.5.6 Импорт и экспорт объектов защиты

Цель:

- экспортировать в файл структуру каталогов, содержащих объекты защиты и используемые в них элементы анализа;
- загружать из файла ранее созданную структуру каталогов, содержащих объекты защиты и используемые в них элементы анализа.

> **Примечание:**
>
> Экспорт и импорт объектов защиты не могут быть выполнены, если конфигурация Системы находится на редактировании. В этом случае будет выведено сообщение об ошибке.

Чтобы экспортировать объекты защиты:

1. Перейдите в раздел **Объекты защиты**.
2. На панели инструментов в левой части рабочей области нажмите на кнопку и в раскрывающемся списке выберите пункт **Экспортировать**.
3. В открывшемся окне укажите, куда требуется сохранить созданный архив.

Сохраненный архив содержит xml-файлы, в которых хранится информация об объектах защиты и используемых в них элементах анализа. При экспорте сохраняется структура каталогов объектов защиты и элементов анализа.

Чтобы импортировать объекты защиты:

1. Перейдите в раздел **Объекты защиты**.
2. На панели инструментов в левой части рабочей области нажмите на кнопку и в раскрывающемся списке выберите пункт **Импортировать**.
3. В открывшемся окне выберите ранее экспортированный файл, который необходимо загрузить.
4. Дождитесь окончания загрузки объектов защиты в Систему.

Примечание:

Если название каталога в файле импорта совпадает с названием каталога в Системе, но различаются пути к каталогу, то каталог из файла импорта добавлен не будет. Если название каталога в файле импорта совпадает с названием каталога в Системе, и путь к каталогу также совпадает, то данные из файла импорта будут объединены с данными, содержащимися в Системе.

Особенности слияния данных при импорте:

1. Для каталога будут добавлены следующие элементы, отсутствующие в Системе:
   а) дочерние каталоги объектов защиты;
   б) объекты защиты.
2. Для объекта защиты будут добавлены следующие элементы, отсутствующие в Системе:
   а) элементы анализа;
   б) условия обнаружения.
3. Для условий обнаружения будут добавлены новые вложенные условия, включая параметры детектирования (для текстовых объектов, бланков и выгрузок из БД).

5.5.7 Активация и деактивация объектов защиты

По умолчанию все создаваемые объекты защиты и их каталоги имеют статус Активный (пиктограмма для объектов защиты и - для каталогов). При необходимости вы можете деактивировать созданный каталог или отдельный объект защиты внутри каталога.

Чтобы деактивировать каталог объектов защиты:

1. На панели инструментов в левой части рабочей области нажмите и в раскрывающемся списке выберите **Деактивировать каталог объектов защиты**.
2. Статус каталога изменится на Неактивный (пиктограмма).

Если вам требуется снова активировать деактивированный каталог, нажмите и в раскрывающемся списке выберите **Активировать каталог объектов защиты**.

Чтобы деактивировать выбранный объект защиты:

1. В левой части рабочей области выберите требуемый каталог.
2. В правой части рабочей области щелчком левой кнопки мыши выделите в списке требуемый объект защиты.
3. На панели инструментов в правой части рабочей области нажмите и в раскрывающемся списке выберите **Деактивировать объект защиты**.
4. Статус объекта защиты изменится на Неактивный (пиктограмма).

Если вам требуется снова активировать деактивированный объект защиты, нажмите и в раскрывающемся списке выберите **Активировать объект защиты**.

Важно!

Объекты защиты и их каталоги могут быть обнаружены в перехваченных данных только в том случае, если они активированы.

5.6 Работа с подсистемой Краулер

Для чего требуется подсистема Краулер?

Работа с подсистемой Краулер требуется для сканирования следующих мест хранения файлов:

- Разделяемые сетевые ресурсы
- Локальные диски рабочих станций
- Файловое хранилище SharePoint 2007/2010/2013

Работа с подсистемой Краулер состоит из следующих действий:

Действие	Описание
Настройка сканера	После того как администратор установит и настроит Систему, пользователь получит доступ к сканеру. Для работы со сканером пользователь может выполнить его настройку
Создание задачи	Для сканирования ресурсов требуется создать задание
Запуск и остановка задачи	Сканирование целевых мест хранения файлов начинается при запуске задачи и прекращается при ее остановке
Редактирование задачи	Изменение настроек задания
Очистка хешей	Сброс сохраненных в Системе контрольных сумм
Просмотр истории запусков	Ознакомление с системной информацией о ходе выполнения задания
Сохранение отчета	Копирование отчета на жесткий диск компьютера

См. также:

- "Раздел Краулер" - о разделе, в котором ведется работа с подсистемой Краулер

5.6.1 Настройка сканера

Цель:
Настроить сканер подсистемы Краулер.

Решение:

1. Перейдите в раздел **Краулер**.
2. На панели инструментов в левой части рабочей области нажмите кнопку **Редактировать сканер**.
3. В правой части рабочей отобразятся атрибуты сканера (см. "Сканер").
4. После изменения хотя бы одного атрибута правее кнопки **Редактировать сканер** отобразится символ , свидетельствующий о том, что задания на сканирование для данного сканера не выполняются.
5. Измените требуемые параметры.
6. Нажмите **Сохранить** для сохранения сделанных изменений или **Отменить** для выхода из режима редактирования без сохранения изменений.

После сохранения конфигурации сканера символ  исчезнет: это значит, что задания на сканирование для данного сканера могут выполняться.

Дополнительная информация:
В значении атрибута **Не отображать следующие SID'ы** перечислены стандартные SID служебных записей. При необходимости, пользователь может добавить в этот список собственные SID и задать маски, используя регулярные выражения.

Пример записи:
`S-1-5-21-.*-(498|502|517|527)`
Данная запись означает, что при отображении информации об объекте в Консоли управления не будет отображаться информация о том, что данный файл доступен учетным записям с любыми SID, начинающимися со строки "S-1-5-21-", имеющими в середине 0 или больше любых букв, цифр, и др. символов, и оканчивающихся на "-498", или "-502", или "-517", или "-527".

Подходящие SID:
`S-1-5-21-12345-ABCDEF-498`
`S-1-5-21-527`

Неподходящие SID:
`1S-1-5-21-12345-ABCDEF-498` - начинается не с "S-1-5-21-"
`S-1-5-21-527` - начинается с "S-1-5-21-", но заканчивается на "527", а не на "-527"
`S-1-5-21-ABCDEF-100` - не заканчивается на "-498", или "-502", или "-517", или "-527".
`S-1-5-21-ABCDEF-502-` - не заканчивается на "-498", или "-502", или "-517", или "-527".
`S-1-6-21-ABCDEF-502` - начинается не с "S-1-5-21-".

> **Примечание:**
>
> Более подробно о формате языка регулярных выражений описано в интернет-статье "Элементы языка регулярных выражений".

5.6.2 Создание задачи

Цель:
Добавить задачу сканирования.

Решение:

1. Перейдите в раздел **Краулер**.
2. На панели инструментов нажмите  **Создать задание**.
3. В правой части рабочей области на вкладке **Подробности** введите атрибуты задания (см. "Задание на сканирование").
4. Обязательны для заполнения следующие поля:
    - **Политика сканирования**;
    - **Сканируемые группы/рабочие станции**;
    - **Расписание**.
5. Нажмите **Сохранить**.

Пример:
Если требуется, чтобы Система присваивала тег *Печатная плата* объектам перехвата, созданным в результате обнаружения текстовых файлов формата TXT, которые содержат словосочетание "печатная плата" и хранятся в корпоративном файловом хранилище SharePointRepo, в БД CorporateDataBase (подразумевается, что файловое хранилище SharePointRepo, включающее БД CorporateDataBase, уже создано в организации), то:

Офицер безопасности должен создать термин с текстом "печатная плата" (см. "Создание терминов") и тег *Печатная плата* (см. "Работа с тегами"), затем применить конфигурацию (см. "Применение конфигурации Системы").
Далее офицер безопасности должен создать задание на сканирование, выбрав в качестве политики сканирования *Файловое хранилище SharePoint* и указав атрибутам следующие значения:

- атрибуту **Адрес БД ресурса** - значение *SharePointRepo*;
- атрибуту **Имя БД ресурса** - значение *CorporateDataBase*.

Затем ОБ должен создать политику, в правиле хранения которой указывает следующие значения атрибутов:

- **Место хранения** - *Файловое хранилище*; атрибутам указываются следующие значения:
    - атрибуту **Введите источник** - значение *SharePointRepo*;
    - атрибуту **Введите путь хранения** - значение *CorporateDataBase*;
- **Теги** - тег *Печатная плата*.

Важно!

Во время выполнения задания даже с использованием прав доменного администратора возможно появление ошибки доступа:

`Ошибка получения каталогов для <адрес_каталога>: Access to the path <адрес_каталога> is denied,`

где `<адрес_каталога>` - абсолютный путь к каталогу проверки.

Такая ошибка может возникнуть, например, если пользователь, являющийся владельцем папки, запретил к ней доступ.

5.6.3 Запуск и остановка задачи

Цели:

1. Запустить задачу сканирования.
2. Остановить задачу сканирования.

Решение:

1. Запуск задачи сканирования.
   a. Перейдите в раздел **Краулер**.
   b. Выделите целевое задание в списке заданий щелчком левой кнопки мыши.
   c. На панели инструментов нажмите  **Запустить задание**.
2. Остановка задачи сканирования.
   a. Перейдите в раздел **Краулер**.
   b. Выделите целевое задание в списке заданий щелчком левой кнопки мыши.
   c. На панели инструментов нажмите  **Остановить задание**.

5.6.4 Редактирование задачи

Цель:
Редактировать задачу сканирования.

Решение:

1. Перейдите в раздел **Краулер**.
2. Выделите целевое задание в списке заданий щелчком левой кнопки мыши.
3. На панели инструментов в левой части рабочей области нажмите  **Редактировать задание**.
4. В правой части рабочей области, в открывшейся форме редактирования, измените атрибуты задания (см. "Задание на сканирование").
5. Нажмите **Сохранить** для сохранения сделанных изменений или **Отменить** для выхода из режима редактирования без сохранения изменений.

5.6.5 Очистка хеша

Справочная информация:
Для оптимизации работы в Crawler предусмотрено хранение **хешей** – контрольных сумм файлов. Если в ходе предыдущего запуска задания сканирования был сохранен хеш какого-либо файла и при очередном запуске того же самого задания сканирования хеш для этого файла не изменился,

это означает, что в данный файл не подвергался изменениям и его не следует отправлять его на обработку на сервер Traffic Monitor. Это позволяет уменьшить нагрузку на канал между Crawler и сервером Traffic Monitor, а также на сам сервер Traffic Monitor, а также исключает дублирование идентичных событий для каждого запуска задания на сканирование.
Особенности хранения базы хешей:

- База хешей сохраняется отдельно для каждого задания сканирования. Следовательно, если какой-либо файл уже был обработан другим заданием, то при создании и запуске другого задания это учитываться не будет.
- Хеш-суммы хранятся для файлов с учетом рабочих станций, на которых эти файлы были обнаружены. Таким образом, если один и тот же файл находится на нескольких рабочих станциях, он будет обрабатываться отдельно для каждой рабочей станции.

Рекомендуется выполнять периодическую очистку базы хешей: например, в том случае, когда изменилась конфигурация Traffic Monitor – то есть согласно изменившейся политике или списку терминов и т.п. решение о том, является ли перехваченный объект потенциальным нарушением, будет приниматься системой по другому алгоритму. В результате очистки базы хешей задание «забудет» о том, что оно когда-либо обрабатывало какие-либо файлы, и будет отправлять для анализа на сервер Traffic Monitor все файлы, соответствующие условиям данного задания.

Цель:
Очистить хеш.

Решение:

1. Перейдите в раздел **Краулер**.
2. Выделите созданное задание в списке заданий щелчком левой кнопки мыши.
3. На панели инструментов нажмите  **Очистить хеши задания**.

5.6.6 Просмотр истории запусков

Справочная информация:
В правой части рабочей области отображается информация о запусках выбранного задания на сканирование.

Цель:
Просмотреть историю запусков задания.

Решение:

1. Перейдите в раздел **Краулер**.
2. Выделите целевое задание в списке заданий щелчком левой кнопки мыши.
3. Просмотрите краткую информацию в правой части рабочей области.
4. Для просмотра расширенной информации о ходе выполнения задания и о параметрах запуска, щелчком левой кнопки мыши выделите запись требуемого запуска в списке.
   Расширенная информация представлена в следующих вкладках:
   - **События сканирования** - вкладка содержит системные сведения о запуске задания на сканирование;
   - **Параметры запуска** - вкладка содержит список атрибутов задания на сканирование (см. "Задание на сканирование").

Для возврата к краткой информации об истории запусков нажмите на ссылку **< Назад**.

5.6.7 Сохранение отчета

Цель:
Сохранить отчет о сканировании.

Решение:

1. Перейдите в раздел **Краулер**.
2. Выделите целевое задание в списке заданий щелчком левой кнопки мыши.
   В правой части рабочей области отобразится история запуска задания.
3. Установите флажок в нужных строках и нажмите кнопку **Скачать xls отчет** в верхней части рабочей области.
4. Откройте сохраненный файл в формате .xls стандартными средствами (например, MS Excel).

5.7 Работа с объектами перехвата

Для чего требуется работа с объектами перехвата?

- отслеживать статистику нарушений политики корпоративной безопасности;
- просматривать сведения по каждому объекту в отдельности;
- отображать объекты перехвата, удовлетворяющие определенным критериям.

Работа с объектами перехвата состоит из следующих действий:

Действие	Описание
Просмотр сводки по нарушениям/нарушителям	Просмотр статистической информации и подборок по событиям
Просмотр событий	Просмотр сведений по каждому объекту перехвата
Работа с выгрузками	Генерирование сводки по нарушениям/нарушителям
Вынесение решения по объекту	Решение по объекту, вынесенное пользователем
Добавление/удаление тега	Добавление тега объекту перехвата
Сохранение события (для SMTP-писем)	Сохранение объекта перехвата в формате EML на диск
Досылка события, находящегося в карантине	Отправление заблокированного сообщения адресату
Создание запросов	Фильтрация объектов перехвата по указанным критериям

См. также:

- "Раздел События" - о разделе, в котором ведется работа с объектами перехвата
- "Раздел "Сводка"" - о разделе, где можно просмотреть сводку по объектам перехвата

5.7.1 Просмотр сводки по нарушениям/нарушителям

Работа ведется в разделе **Сводка** (см. "Раздел Сводка")

Цель:
Просмотреть сводку по нарушениям/нарушителям.

Решение:

1. Перейдите в раздел **Сводка**.
2. Настройте панель инструментов (см. "Создание панели").
3. Добавьте и настройте требуемый виджет (см. "Создание виджета" и "Настройка виджета").
4. Изучите сводку, представленную на виджете.

5.7.1.1 Создание панели

Цель:
Создать панель, на которой будут располагаться виджеты.

Решение:

1. Перейдите в раздел "**Сводка**".
2. В левом верхнем углу рабочей области нажмите  **Добавить**.
3. Укажите название для новой панели.
4. Нажмите **Сохранить**.

Дополнительные сведения:

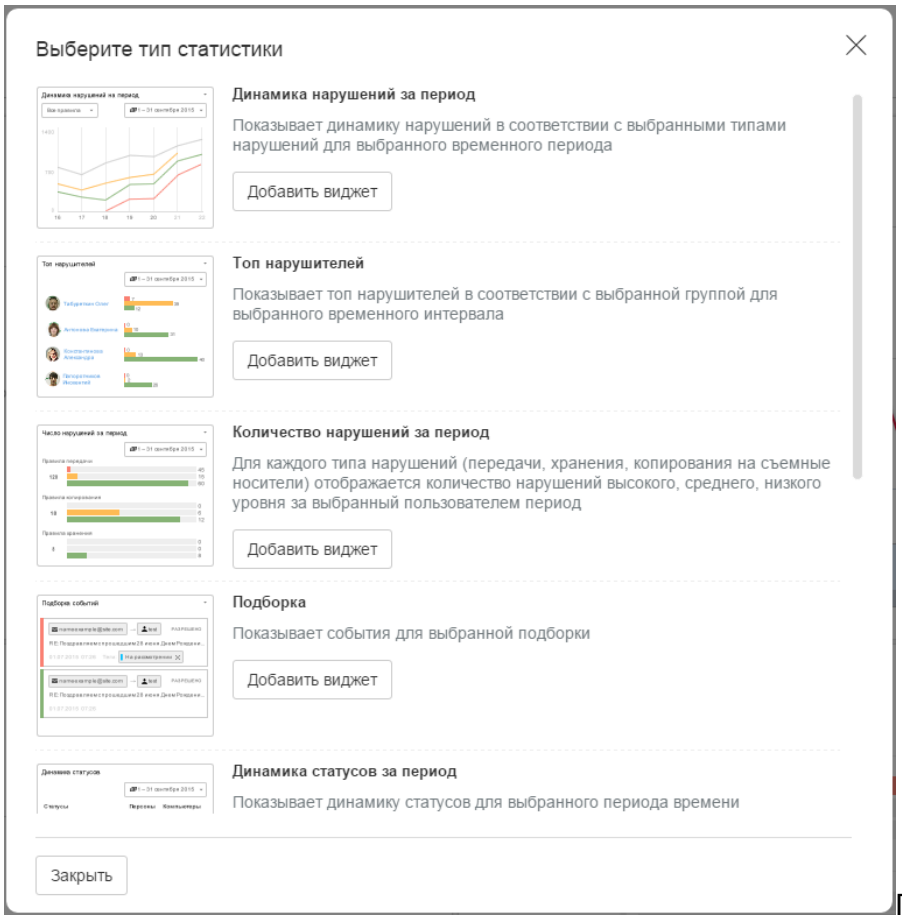
- Наполнение панели описано в статье "Создание виджета".
- Для удаления панели перейдите на панель, которую требуется удалить и нажмите  на вкладке с названием панели. В окне подтверждения нажмите **Удалить**.

5.7.1.2 Создание виджета

Цель:
Создать виджет на панели сводки.

Решение:

1. Перейдите в раздел "**Сводка**".
2. Перейдите на панель, на которую требуется добавить виджет, или создайте новую панель (см. "Создание панели").
3. Нажмите **Добавить виджет**.
4. В открывшемся окне **Выберите тип статистики** выберите требуемый виджет и нажмите **Добавить виджет** под его описанием.



Подробное о типах виджетов см. в статье "Виджеты сводки".
Вы можете добавить на панель несколько виджетов подряд. Для этого нажммите **Добавить виджет** под всеми виджетами, которые вы хотите добавить.
Вы можете добавить несколько виджетов одного типа, а затем настроить их на отображение различных типов данных: например, несколько виджетов с типом **Подборка** для отображения событий по результатам запросов (о создании фильтров событий см. статьи "Создание запроса в стандартном режиме" и "Создание запроса в расширенном режиме").

5. Нажмите **Закрыть** или используйте кнопку ✕ в правом верхнем углу окна.
6. Настройте добавленные виджеты для отображения требуемых данных: см. "Настройка виджета".

Дополнительные сведения:

1. Вы можете перемещать плитки виджета, располагая их в удобном порядке. Для этого:
   a) Наведите указатель мыши на заголовок плитки, чтобы стандартный вид курсора изменился на вид курсора перемещения (четырехконечная стрелка).
   b) Зажмите левую клавишу мыши и, удерживая ее зажатой, перемещайте плитку по рабочей области, пока целевая позиция плитки не выделится пунктирной линией.
   c) Отпустите левую клавишу мыши.

2. Чтобы отредактировать виджет, в правом верхнем углу нажмите ▾ и в раскрывающемся списке выберите **Редактировать**. В открывшемя окне **Общие настройки виджета** измените требуемые параметры, после чего нажмите **Сохранить**.

3. Чтобы удалить виджет, в правом верхнем углу нажмите ▾ и в раскрывающемся списке выберите **Удалить**. В окне подтверждения нажмите **Да**.

5.7.1.3 Настройка виджета

Цель:
Настроить виджет.

Решение:

1. Перейдите в раздел "**Сводка**" и откройте требуемую панель.
2. Выберите требуемый виджет или добавьте новый (см. "Создание виджета").
3. При помощи элементов интерфейса, расположенных в верхней части виджета, вы можете указать такие настройки как тип правил, нарушения которых будут отображаться на виджете, и интересующий вас период времени.
4. Для изменения остальных настроек нажмите кнопку и в раскрывающемся списке нажмите **Редактировать**.
5. В открывшемся окне **Общие настройки виджета** измените требуемые параметры (см. "Виджеты сводки").
6. Нажмите **Сохранить**.

,

5.7.2 Просмотр событий

Цель:
Просмотреть информацию по объекту перехвата.

Решение:

1. Перейдите в раздел **События** (см. "Раздел События").
2. Примените фильтрацию событий, создав и выполнив запрос (см. "Создание запросов").

> **Примечание:**
>
> В списке отображаются последние 10 000 событий. События отсортированы по ID-номеру события в порядке убывания.

3. Если требуется, измените список полей просмотра событий (см. "Выбор полей просмотра событий").
4. Просмотрите информацию по событию в плитке события или в строке таблицы (см. п.3 на схеме в статье "Раздел События ").
5. При необходимости используйте краткую и детальную формы просмотра события.

5.7.2.1 Создание запросов

Цель:
Создать запрос, позволяющий отфильтровать объекты перехвата.

Решение:

1. Перейдите в раздел **События** (см. "Раздел События").
2. Выберите запрос из раскрывающегося списка запросов в верхней строке левой части рабочей области или создайте новый.

> **Примечание:**
>
> Доступны два способа создания запроса: в стандартном режиме и в расширенном режиме.

3. Примените запрос по событиям, нажав **Выполнить запрос** (при создании запроса вы можете также использовать кнопку **Сохранить и выполнить**).

> **Примечание:**
>
> Чтобы скрыть результаты выполнения запроса, справа от названия запроса в списке запросов нажмите кнопку .

См. также:

- "Создание запроса в стандартном режиме" - о создании стандартного запроса
- "Создание запроса в расширенном режиме" - о создании расширенного запроса

5.7.2.1.1 Создание запроса в стандартном режиме

Цель:
Создать запрос для поиска событий, удовлетворяющих заданным условиям.

Решение:

1. Перейдите в раздел **События**.
2. На панели инструментов в верхней строке левой части рабочей области нажмите **Добавить запрос**.
3. В раскрывающемся списке выберите **Обычный запрос**. В правой части рабочей области откроется форма создания запроса.
4. В поле **Название** введите название запроса.
5. На вкладке **Условие** заполните поля, по которым будет осуществляться поиск (см. "Условие").
6. На вкладке **Поля просмотра** выберите атрибуты, значения которых будут показаны для найденных событий (см. "Поля просмотра").

7. Если вы хотите открыть доступ на просмотр и редактирование запроса другими пользователями, то на вкладке **Параметры доступа** снимите флажок в поле **Запрос доступен только владельцу запроса** (по умолчанию флажок установлен).
8. Нажмите:
    - **Сохранить** - чтобы сохранить запрос.
    - **Сохранить и выполнить** - чтобы сохранить и выполнить запрос.

Примечание.

Для более гибкой настройки условий поиска вы можете воспользоваться расширенным режимом.

Пример:

Если требуется, чтобы Система отображала события с уровнем нарушения *Высокий* и присвоенной политикой *Юридическая документация*:
Офицер безопасности создает запрос в стандартном режиме и указывает атрибуту **Уровень нарушения** значение *Высокий*, а атрибуту **Политика** - значение *Юридическая документация*.

Дополнительные сведения:
Редактирование и удаление запроса выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.7.2.1.2 Создание запроса в расширенном режиме

Цель:
Выполнить гибкую настройку условий поиска событий.

Решение:

1. Перейдите в раздел **События**.
2. На панели инструментов, в верхней строке левой части рабочей области, нажмите + **Добавить запрос**.
3. В раскрывающемся списке выберите **Расширенный запрос**. Откроется окно создания запроса.
4. В поле **Название** укажите название запроса.
5. На вкладке **Условие**, в раскрывающемся списке **Добавить условие**, выберите параметры, по которым будет осуществляться поиск.
6. По умолчанию добавленные атрибуты связаны операцией конъюнкции (логическое "И"). Для изменения типа операции левой кнопкой мыши нажмите на пиктограмму and. При этом пиктограмма изменится на or, что соответствует операции дизъюнкции (логическое "ИЛИ").
7. Для отделения атрибутов, связанных операцией конъюнкции (логическое "И"), от атрибутов, связанных операцией дизъюнкции (логическое "ИЛИ"), используйте элемент **Группа параметров** (см. "Расширенный режим").
8. На вкладке **Поля просмотра**, выберите атрибуты, значения которых будут показаны для событий, удовлетворяющих условиям запроса (см. "Поля просмотра").

9. Если вы хотите открыть доступ на просмотр и редактирование запроса другими пользователями, то на вкладке **Параметры доступа** снимите флажок в поле **Запрос доступен только владельцу запроса** (по умолчанию флажок установлен).

10. Нажмите **Сохранить**.

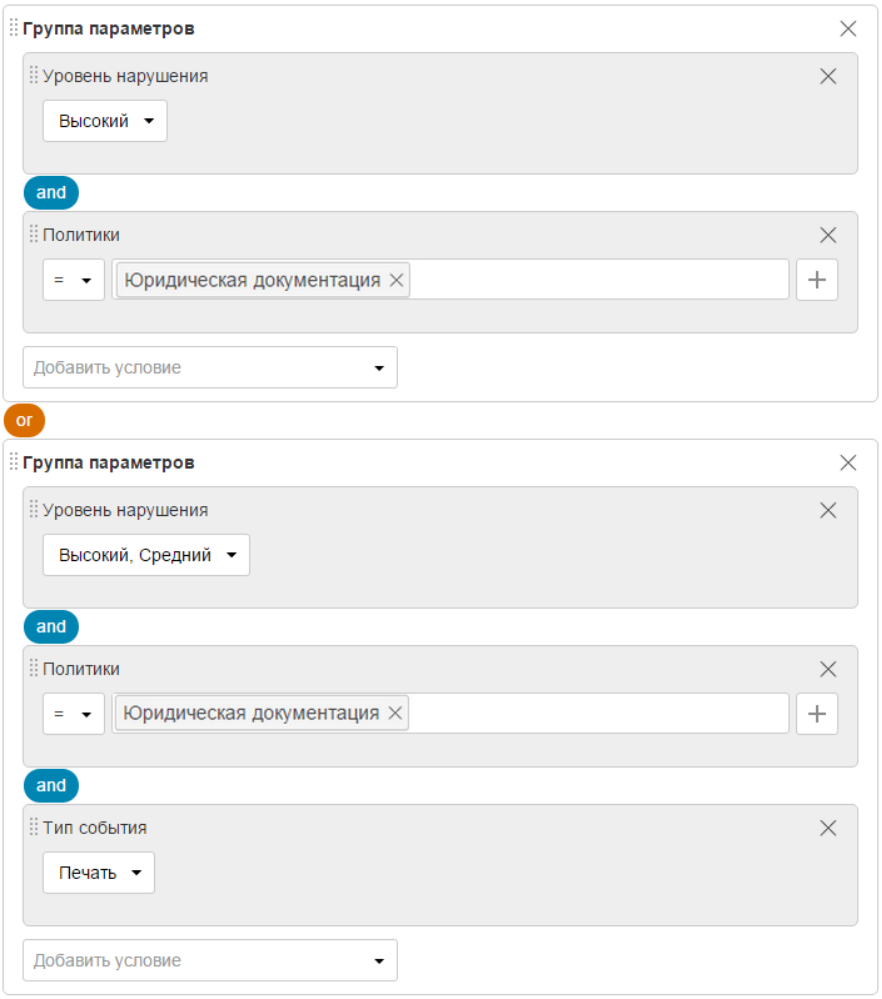
Пример 1:

Если требуется, чтобы Система отображала события:

- с уровнем нарушения *Высокий* и присвоенной политикой *Юридическая документация*;
- с уровнями нарушения *Высокий* и *Средний*, с присвоенной политикой *Юридическая документация* и типом *Печать*:

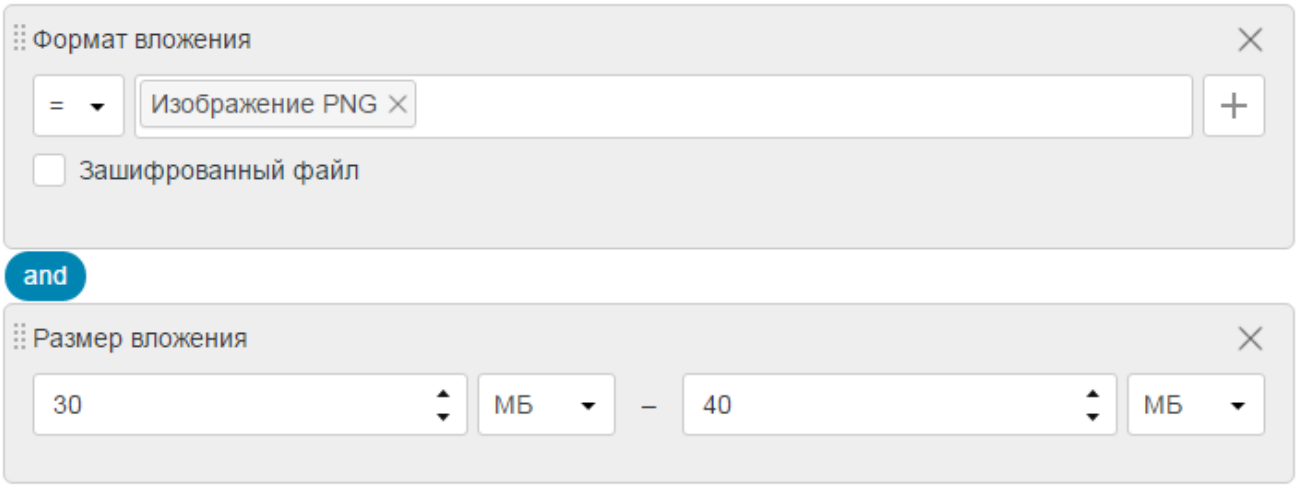
Офицер безопасности создает запрос в расширенном режиме и в качестве атрибутов указывает две группы параметров, связанных операцией дизъюнкции (см. рисунок ниже):

- В первой группе параметров блоке содержатся атрибуты со значениями:
  - **Уровень нарушения** - *Высокий*;
  - **Политика** - *Юридическая документация*;
- Во второй группе содержатся атрибуты со значениями:
  - **Уровень нарушения** - *Высокий* и *Средний*;
  - **Политика** - *Юридическая документация*;
  - **Тип события** - *Печать*;
- Атрибуты внутри групп связаны операцией конъюнкции.

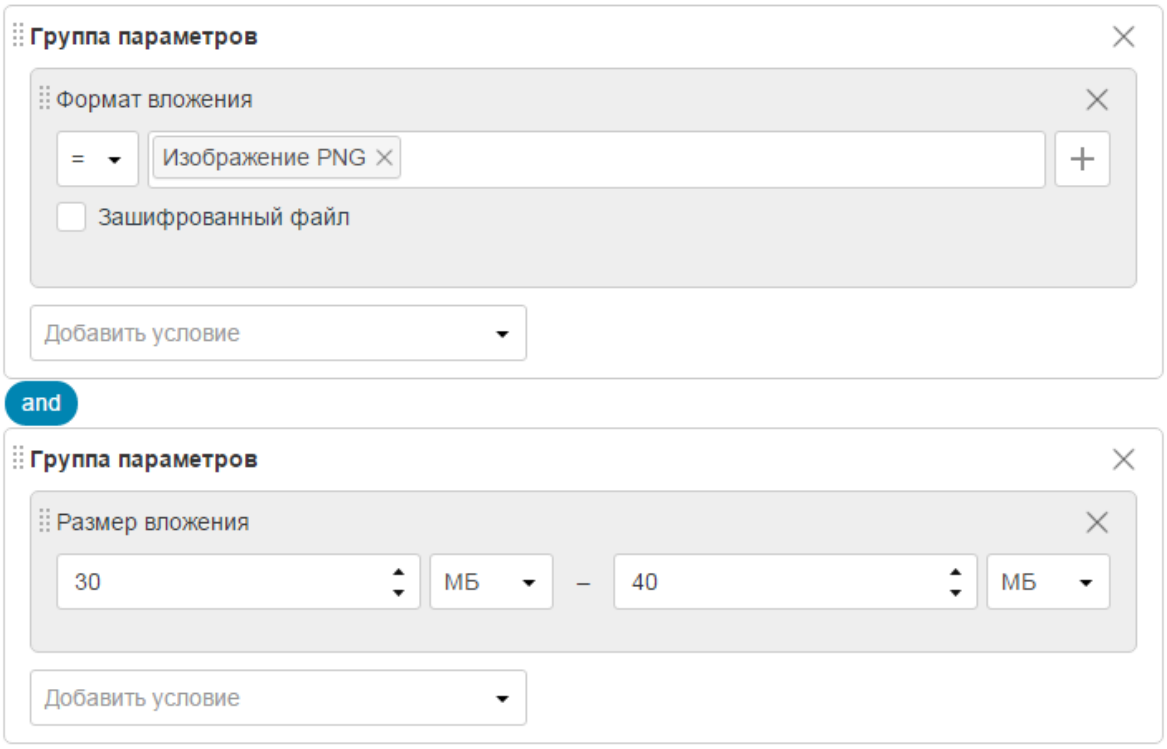


Пример 2:
Если условия заданы для вложений объекта, то при наличии у объекта нескольких вложений условия будут применяться следующим образом:

1. Если несколько условий объединены с помощью операции конъюнкции (логическое "И") внутри одной группы параметров, то после выполнения запроса будут показаны объекты, у которых хотя бы одно вложение удовлетворяет всем заданным условиям. В примере ниже при выполнении запроса будут показаны объекты, у которых хотя бы одно вложение имеет формат PNG и размер от 30 до 40 МБ.



2. Если каждое условие содержится в отдельной группе параметров и группы объединены между собой с помощью операции конъюнкции (логическое "И"), то после выполнения запроса будут показаны объекты, у которых каждое условие выполняется для какого-либо из вложений. В примере ниже при выполнении запроса будут показаны объекты, у которых хотя бы одно вложение имеет формат PNG и хотя бы одно из вложений имеет размер от 30 до 40 МБ.

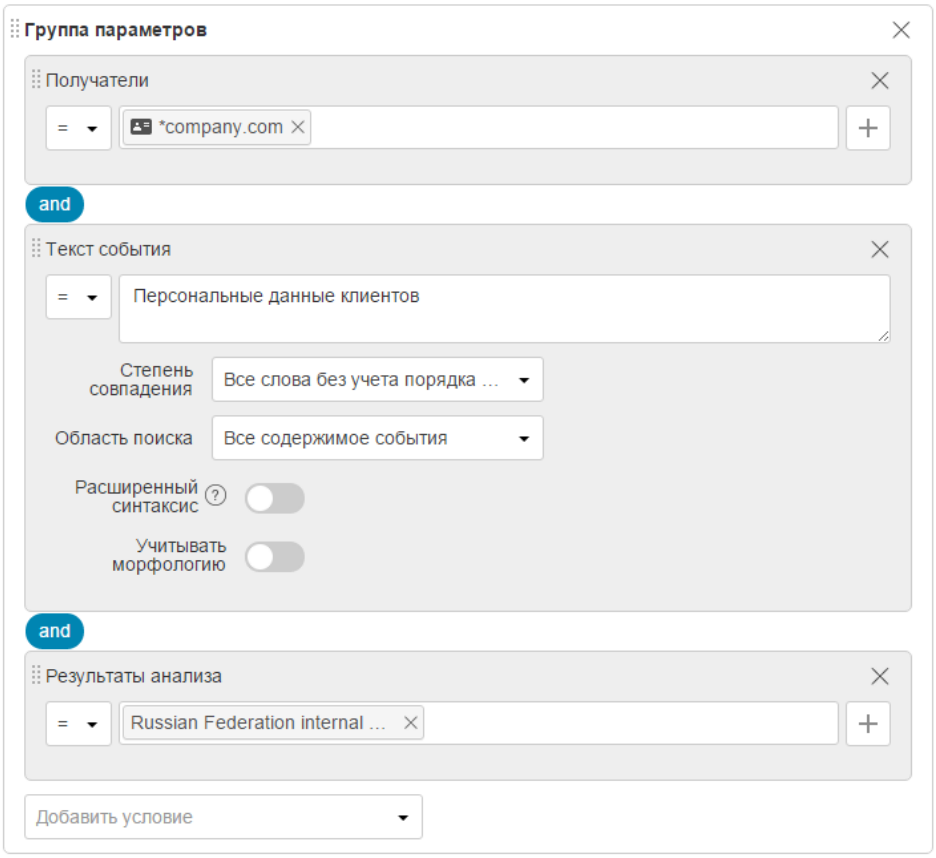


Пример 3:
Если требуется, чтобы Система отображала события:

- пересылаемые внутри компании;
- не содержащие слова *Персональные данные клиентов* в тексте события;
- содержащие номера паспортов:

Офицер безопасности создает запрос в расширенном режиме и указывает внутри группы параметров следующие атрибуты, связанные операцией конъюнкции (см. рисунок ниже):

- `Получатели` - **company.com*;
- `Текст события` - *"Персональные данные клиентов"*, при этом выбрана степень совпадения *Все слова без учета порядка следования и расстояния между ними* и к атрибуту применен параметр отрицания;
- `Область поиска` - *"Все содержимое события"*;
- `Результаты анализа` - текстовый объект *"Паспорт гражданина РФ"*.



Дополнительные сведения:
Редактирование и удаление запроса выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.7.2.1.3 Использование расширенного синтаксиса

Цель:
Настроить поиск по тексту события с использованием расширенного синтаксиса.

Решение:

1. Перейдите в расширенный режим создания запроса.
2. На вкладке **Условие**, в раскрывающемся списке **Добавить условие**, выберите параметр **Текст события**.

3. Включите настройку **Расширенный синтаксис**.
4. В поле **Условие** введите искомый текст, используя логические операторы: "|", "-", "!", "( )" и другие.
5. Укажите остальные параметры запроса (подробнее см. "Создание запроса в расширенном режиме").
6. Нажмите **Сохранить**.

Подробную информацию о создании запросов с использованием логических операторов Вы можете найти в Интернет-статье о языке поисковых запросов Sphinx.

Примечание:

Обратите внимание, что область, в которой будет выполняться поиск, указывается в явном виде в поле **Область поиска** (см. "Поиск по тексту события"). Указывать область поиска с помощью операторов языка Sphinx не требуется.

Пример:

Если требуется, чтобы в тексте события:

- содержались слова *"персональные данные клиентов"* или *"личные данные клиентов"*;
- не содержалась фраза *"конфиденциальная информация"*,

Офицер безопасноти может создать следующий запрос, используя расширенный синтаксис:

```
(персональные| личные) данные клиентов -"конфиденциальная информация"
```

5.7.2.2 Выбор полей просмотра событий

Справочная информация:
По умолчанию в плитке события (или в строке таблицы - в зависимости от выбранного стиля) отображаются все атрибуты события.

Цель:
Выбрать отображаемые атрибуты объектов перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Выполните одно из следующих действий:
   - отредактируйте уже созданный запрос. Для этого нажмите  **Редактировать запрос**;
   - создайте новый запрос.

Примечание:

Доступны два способа создания запроса: в стандартном режиме и в расширенном режиме.

3. В правой части рабочей области перейдите на вкладку **Поля просмотра**.
4. Перенесите все целевые атрибуты в правое поле, а все нецелевые - в левое (см. "Поля просмотра"):
   - Щелчком левой кнопки мыши выделите запись в левом поле, чтобы перенести ее в правое поле;
   - Щелчком левой кнопки мыши выделите запись в правом поле, чтобы перенести ее в левое поле.
5. Нажмите:
   - **Сохранить** - чтобы сохранить изменения;
   - **Сохранить и выполнить** - чтобы сохранить изменения и выполнить фильтрацию с учетом заданных параметров запроса.

5.7.2.3 Просмотр краткой формы события

Цель:
Просмотреть краткую информацию по объекту перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Создайте запрос либо запустите выполнение ранее созданного запроса (см. "Создание запросов").
3. Выделите плитку целевого события в списке (или строку события в таблице событий).
4. Нажмите кнопку ⌄ в правой части рабочей области для открытия краткой информации о событии. Чтобы скрыть информацию о событии, используйте кнопку ⌃.
5. Просмотрите краткую информацию о событии в правой части рабочей области.

См. также:

- "Краткая форма просмотра события" - о форме просмотра общей информации о событии
- "Просмотр детальной формы события" - о просмотре расширенной информации о событии

5.7.2.4 Просмотр детальной формы события

Цель:
Просмотреть детальную информацию по объекту перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Создайте запрос либо запустите выполнение ранее созданного запроса (см. "Создание запросов").

3. Выделите плитку целевого события в списке (или строку события в таблице событий). В правой части рабочей области отобразится краткая форма просмотра события.
4. Для открытия детальной формы просмотра нажмите **Подробнее** в верхней строке правой части рабочей области.
5. В открывшемся окне просмотрите детальную информацию о событии:
    - вкладка **Общая информация** отображает атрибуты события (например, **Отправители**, **Получатели**, **Теги**, **Политики**, **Дата отправки**, **Дата перехвата**);
    - вкладка **Объекты защиты** отображает объекты защиты, обнаруженные в событии; сработавшие технологии, входящие в эти объекты защиты; и каталоги, в которых состояли объекты защиты на момент перехвата;
    - вкладка **Сообщения обработки** отображает ошибки, возникшие в процессе обработки события.
6. Для просмотра информации на вкладках нажмите значок . Чтобы скрыть панель информации, нажмите .
7. Для закрытия детальной формы просмотра используйте кнопку **Закрыть** или стандартную кнопку закрытия в правом верхнем углу окна.

См. также:

- "Детальная форма просмотра события" - о форме просмотра расширенной информации о событии
- "Просмотр краткой формы события" - о форме просмотра общей информации о событии

5.7.3 Работа с выгрузками сводки

Цель:
Создавать и просматривать выгрузки сводки.

Решение:
Решение состоит из следующих действий:

Действие	Описание
Создание выгрузки сводки	Формирование выгрузки сводки по панели
Просмотр выгрузки сводки	Просмотр файлов, содержащих сгенерированную выгрузку - в форматах PDF или HTML

См. также:

- "Выгрузка сводки" - о разделе, в котором ведется работа с выгрузками

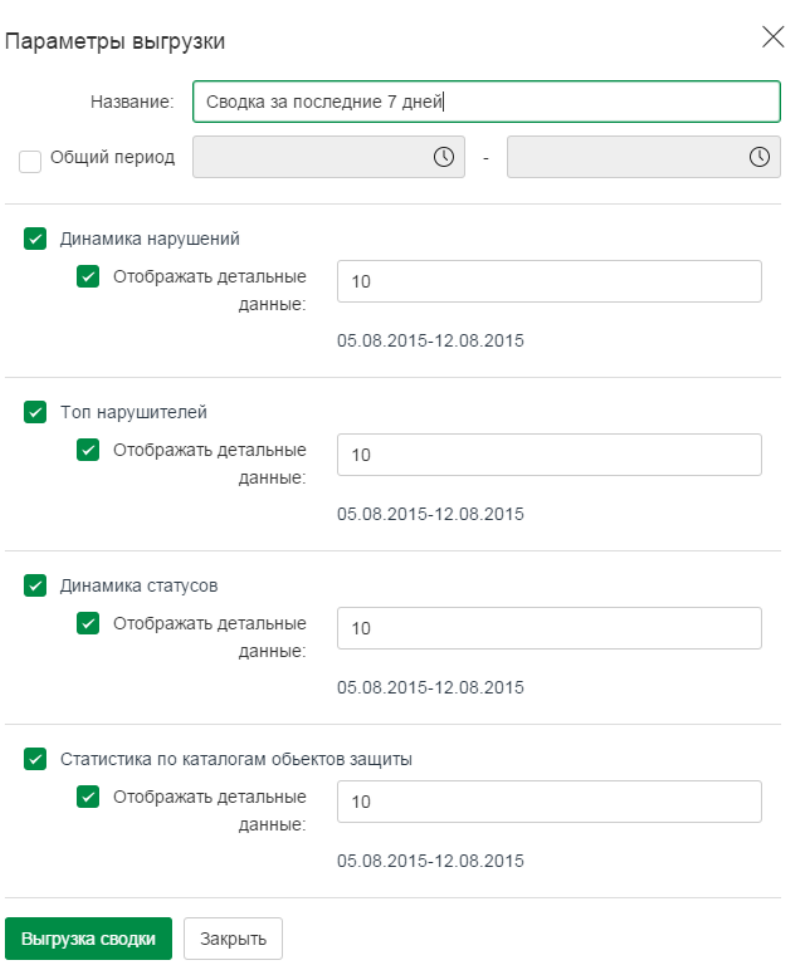
5.7.3.1 Создание выгрузки сводки

Цель:
Создать выгрузку сводки по объектам перехвата.

Решение:

1. Перейдите в раздел "**Сводка**".

2. В правом верхнем углу рабочей области нажмите **Выгрузить**.
3. В открывшемся окне укажите атрибуты выгрузки (см. "Выгрузка сводки").



4. Убедитесь, что флажками отмечены все виджеты, данные которых вы хотите включить в выгрузку.

> **Примечание.**
>
> Данные виджета "Подборка" в выгрузке сводки не отображаются.

5. Если вы хотите вручную указать период, за который будет сформирована выгрузка, установите флажок в поле **Общий период** и введите начальную и конечную дату. Если данная настройка не выбрана, то для каждого виджета, включенного в отчет, выгрузка будет сформирована за период, указанный в настройках виджета.
6. Нажмите **Выгрузка сводки**.

В правом верхнем углу рабочей области будет отображаться информация о ходе генерации выгрузки.

После завершения генерации будет предложено открыть выгрузку в формате PDF или HTML.

Все созданные выгрузки сохраняются в Системе и доступны по нажатию кнопки **Посмотреть список выгрузок** в правом верхнем углу рабочей области. Подробнее см. "Просмотр выгрузок сводки".

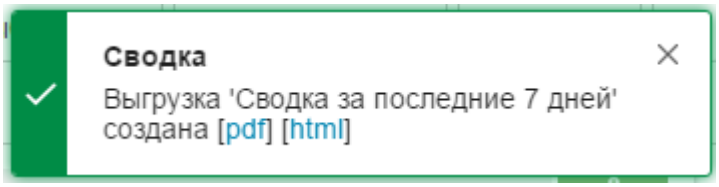
Примечание:

Если виджет, по которому была сформирована выгрузка, будет изменен либо удален с панели, то уже готовая выгрузка изменена не будет.

5.7.3.2 Просмотр выгрузки сводки

Цель:
Просмотреть созданную выгрузку сводки по объектам перехвата.

Решение:
По завершении генерации выгрузки в правом верхнем углу рабочей области отображается информационное сообщение с предложением открыть выгрузку в формате PDF или HTML.



Нажмите на ссылку **pdf** или **html**, чтобы открыть выгрузку в новом окне браузера. Также вы можете сохранить, отправить или распечатать созданную выгрузку стандартными средствами вашего браузера и операционной системы.
Все сгенерированные выгрузки сохраняются в Системе и доступны по нажатию кнопки **Посмотреть список выгрузок**.

Чтобы просмотреть список:

1. Перейдите в раздел "**Сводка**".
2. В правом верхнем углу рабочей области нажмите кнопку **Посмотреть список выгрузок**.
3. В открывшемся окне **Выгрузки** отображается список сгенерированных выгузок. В столбце **Формат выгрузки** напротив требуемой выгрузки, нажмите:
   - **pdf** - если требуется отобразить выгрузку сводки в формате PDF;
   - **html** - если требуется отобразить выгрузку сводки в формате HTML.

Примечание.

Вы можете отсортировать выгрузки в списке по дате создания, а также воспользоваться полем **Поиск** для поиска нужной выгрузки по названию.

4. Откроется новая вкладка браузера, где будет показана выбранная выгрузка.

5.7.4 Вынесение решения по объекту

Цель:
Вынести решение, является ли объект нарушением.

Решение:

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите нужное событие в списке.
3. На панели инструментов в левой части рабочей области нажмите:
   -  **Нарушение** - для событий, нарушающих политику корпоративной безопасности. При этом, если для события был назначен вердикт *Поместить на карантин*, то значение вердикта изменится на *Заблокировано*.
   -  **Нет нарушения** - для событий, не являющихся нарушением политики корпоративной безопасности. При этом, если для события был назначен вердикт *Поместить на карантин*, то значение вердикта изменится на *Разрешено*.

     Важно!

     Если используется режим *Блокировка*, то SMTP-письма, перемещенные Системой в карантин, в результате принятия этого решения будут отправлены получателю, а отправитель письма получит уведомление. Подробнее см. "Досылка заблокированного события".

   -  **Решение не принято** - если на данный момент пользователь не принял решение, нарушает ли событие политику корпоративной безопасности.
   -  **Требуется дополнительная обработка** - если для принятия решения требуются дополнительные действия.

См. также:

- "Ретроспективный анализ данных, решение пользователя по объекту" - о вынесении пользовательского решения.

5.7.5 Добавление и удаление тега

Цель:
Добавить тег объекту перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите целевое событие.
3. На панели инструментов для событий нажмите  **Установить тег**.
4. В открывшемся окне выберите требуемый тег, установив для него флажок.

5. Нажмите **Сохранить**.

Для удаления тега нажмите на крестик рядом с названием тега в плитке события.

См. также:

- "Теги" - об интерфейсе раздела Консоли управления, в котором ведется работа с тегами
- "Работа с тегами" - о порядке наполнения справочника тегов

5.7.6 Сохранение события (для SMTP-писем)

Цель:
Сохранить объект перехвата (SMTP-письмо).

Решение:

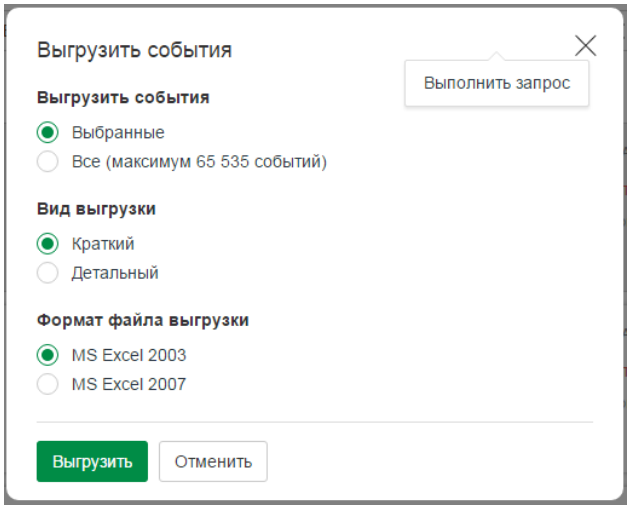
1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите целевое событие.
3. В краткой форме просмотра события, расположенной в правой части рабочей области, нажмите .
   Начнется скачивание файла. После окончания загрузки вы можете открыть файл события и просмотреть его содержимое.

5.7.7 Выгрузка события

Цель:
Сохранить информацию о событиях на диск компьютера.

Решение:

1. Зайдите в раздел **События**.
2. Нажмите на значок табличной формы просмотра .
3. Выполните запрос для получения объектов.
4. Выделите в списке событие, которое вы хотите выгрузить. Чтобы выделить несколько событий, используйте клавиши Shift или Ctrl.
   Если вы хотите сформировать выгрузку для всех имеющихся событий, пропустите этот пункт.
5. На панели инструментов нажмите и в раскрывшемся списке выберите **Выгрузить события**.
   Откроется диалоговое окно **Выгрузка событий**.



6. Убедитесь, что для параметра **Выгрузить события** установлено верное значение: **Выбранные**, если вы хотите выгрузить отдельные события, или **Все**, если вы хотите сформировать выгрузку для всех найденных событий.
7. Укажите остальные параметры выгрузки: вид (Краткий или Детальный) и формат файла выгрузки (MS Excel 2003 или MS Excel 2007).
8. Нажмите **Выгрузить**.

По завершении операции в правом верхнем углу будет отображено уведомление. Чтобы открыть новый или существующий файл выгрузки, нажмите **скачать**.

5.7.8 Досылка события, находящегося в карантине

Справочная информация:
Если персона отправила SMTP-письмо, признанное потенциальным нарушением политики безопасности и перемещенное Системой в карантин (в Системе для SMTP-трафика применяется транспортный режим *Блокировка*), офицер безопасности может затем пересмотреть решение Системы и разрешить отправку письма. В этом случае будет выполнена досылка письма, а отправитель письма получит уведомление.

Цель:
Выполнить досылку письма, помещенного Системой в карантин.

Решение:

> **Важно!**
>
> Досылка письма возможна только для событий, имеющих вердикт *Карантин*. События с вердиктом *Заблокировано* дослать невозможно.

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите целевое событие.
3. На панели инструментов в левой части рабочей области нажмите  **Нет нарушения**.

См. также:

- "Ретроспективный анализ данных, решение пользователя по объекту" - о вынесении пользовательского решения;
- "Вынесение решения по объекту" - о действиях офицера безопасности по принятию возможных решений по объекту.

5.8 Настройка реакций Системы

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Справочная информация:
Реакции Системы - это действия, выполняемые Системой при обнаружении нарушений политики корпоративной безопасности. Эти действия задаются в правилах при создании политик защиты данных и политик контроля персон (см. "Раздел Политики"). Также в Системе имеются предустановленные политики (см. "Политики по умолчанию").
В процессе работы Системы может возникнуть ситуация, когда подсистема анализа и принятия решений не может использовать политику: например, политика не создана или была удалена, при выполнении политики произошла ошибка. В этом случае объектам не назначается никаких атрибутов, а в детальной форме просмотра событий, на вкладке **Сообщения обработки**, отображаются сообщения о возникших в процессе обработки ошибках (см. "Детальная форма просмотра событий").

Для чего требуется настройка реакций Системы:
Для того чтобы при нарушении корпоративной политики безопасности (например, отправка конфиденциального документа за пределы компании) и нецелевом использовании рабочего времени (например, просмотр развлекательных интернет-сайтов с рабочего компьютера) Система выполняла:

- отправку уведомлений нарушителям и информирование пользователей Консоли управления;
- назначение вердикта объекту перехвата;
- присвоение объекту перехвата уровня нарушения, тегов и статуса.

Настройка реакций Системы состоит из следующих действий:

Действие	Описание
Создание политики защиты данных	Политика защиты данных представляет собой набор правил передачи, контроля и хранения. Позволяет указать данные, действия с которыми могут приводить к срабатыванию правил политики.
Создание политики контроля персон	Позволяет указать список контролируемых персон, действия которых могут приводить к срабатыванию правил политики.

Действие	Описание
Создание правила	Определение, что является нарушением правила политики, и какие действия необходимо выполнить в случае нарушения
Отправка уведомлений о сработавшем правиле	При срабатывании правила Система отправляет уведомление указанным пользователям Консоли

Примечание.

При наличии большого числа политик в Консоли управления вы можете отфильтровать список политик по заданным критериям (подробнее см. "Фильтрация списка политик").

См. также:

- "Раздел Политики" - о разделе, в котором ведется работа с политиками

5.8.1 Общие сведения о политиках

В этом разделе описан порядок применения настроенных политик Системы (т.е. совокупностей правил, в соответствии с которыми проводится анализ и обработка объектов) к событиям (объектам перехвата сетевого трафика).

Политики в Системе делятся на две группы:

1. Политики защиты данных - позволяют настроить правила передачи, копирования и хранения для защищаемых данных.
2. Политики контроля персон - позволяют отслеживать действия отдельных персон и их групп.

К перехваченным объектам сначала применяются все активные политики защиты данных, затем - активные политики контроля персон.

Система применяет политики к событиям в следующем порядке:

1. **Событие по очереди проверяется на соответствие всем активным политикам (вначале - политикам защиты данных, затем - политикам контроля персон)**
2. **Если политика сработала на событии, рассматриваются суб-события**
3. **Для каждого суб-события отбираются правила, которым они соответствуют (которые срабатывают на данное суб-событие)**
4. **Правила, которые сработали, разделяются на суб-правила**
5. **Из суб-правил, соответствующих событию, выбираются самые приоритетные**
6. **К объекту перехвата применяются действия, заданные в сработавших суб-правилах самого высокого приоритета**
7. **Если остались суб-события, которым не соответствует ни одно правило, выполняются действия по умолчанию (в случае, если они указаны для данного типа правил)**

Подробнее о процессах, происходящих при этом:

- Разбиение события на суб-события

- Разбиение правил на суб-правила
- Определение приоритетного суб-правила
- Порядок применения действий согласно отобранным приоритетным правилам
- Пример применения политики

5.8.1.1 Разбиение события на суб-события

В результате обработки события Система присваивает ему ряд атрибутов (см. "Анализ объекта и вынесение решения по объекту"). Если какой-либо атрибут события получил несколько значений (например, несколько получателей SMTP-письма, или соответствие текста POST-запроса нескольким категориям и т.п.), то Система рассматривает это событие как совокупность нескольких суб-событий с уникальными значениями атрибутов.
Например, если перехваченное событие имеет следующие атрибуты:

Отправитель	**Получатель**	**Протокол**	**Время**
Персона: Иванов, Персона: Петров	Персона: Сидоров, Персона: Петров, Персона: Иванов	Skype	09:23

то оно подразделяется на следующие суб-события:

Отправитель	**Получатель**	**Протокол**	**Время**
Персона: Иванов	Персона: Сидоров	Skype	09:23
Персона: Иванов	Персона: Петров	Skype	09:23
Персона: Иванов	Персона: Иванов	Skype	09:23
Персона: Петров	Персона: Сидоров	Skype	09:23
Персона: Петров	Персона: Петров	Skype	09:23
Персона: Петров	Персона: Иванов	Skype	09:23

5.8.1.2 Разбиение правил на суб-правила

При применении правил действующей политики также применяется разбиение правил на суб-правила для выявления суб-правил с наивысшим приоритетом.
Для этого из всех правил политики отбираются правила, которые соответствуют перехваченному событию по атрибутам: ***Отправитель***, ***Получатель***, ***Протокол***, например:

Отправитель	**Направление**	**Получатель**	**Протокол**	**Время**	**Реакция**
Группа: Юристы, Персона: Иванов, Персона: Петров	->	Группа: Маркетинг, Персона: Сидоров	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Логистики	->	Группа: Продаж, Группа: Доставки	Skype	10:00-19:00	Уведомить: Петрова, Уровень нарушения: Средний

Отправитель	Направление	Получатель	Протокол	Время	Реакция
Группа: Финансисты	-> <-	Группа: Юристы, Группа: Продаж			Уведомить: Белова, Уровень нарушения: Высокий

Далее производится разбиение на суб-правила по каждой паре отправителя-получателя, при этом при двусторонней передаче данных (например, сессия сообщений в чате) производится разбиение с унификацией направления отправки:

Отправитель	Направление	Получатель	Протокол	Время	Реакция
Группа: Юристы	->	Группа: Маркетинг	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Юристы	->	Персона: Сидоров	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Иванов	->	Группа: Маркетинг	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Иванов	->	Персона: Сидоров	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Петров	->	Группа: Маркетинг	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Петров	->	Персона: Сидоров	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Логистики	->	Группа: Продаж	Skype	10:00-19:00	Уведомить: Петрова, Уровень нарушения: Средний
Группа: Логистики	->	Группа: Доставки	Skype	10:00-19:00	Уведомить: Петрова, Уровень нарушения: Средний
Группа: Финансисты	->	Группа: Юристы			Уведомить: Белова, Уровень нарушения: Высокий
Группа: Финансисты	->	Группа: Продаж			Уведомить: Белова, Уровень нарушения: Высокий
Группа: Юристы	->	Группа: Финансисты			Уведомить: Белова, Уровень нарушения: Высокий
Группа: Продаж	->	Группа: Финансисты			Уведомить: Белова, Уровень нарушения: Высокий

5.8.1.3 Определение приоритетного суб-правила

Приоритет правила определяется исходя из (в порядке убывания):

1. Приоритетной пары отправитель-получатель;
2. Наличия в правиле условия по времени и протоколу;
3. Наличия в правиле условия по времени;

4. Наличия в правиле условия по протоколу.

Приоритетной парой отправитель-получатель считается та, которая имеет наибольшее суммарное количество баллов отправителя и получателя:

Отправитель/Получатель	Количество баллов
Контакт	10000
Персона	5000
Группа	2500
Домен	1250
URL	600
Список ресурсов	300
Отрицание Список ресурсов	150
Отрицание URL	75
Отрицание Домен	35
Отрицание Группа	15
Отрицание Персона	7
Отрицание Контакт	3
Любой	1

Например, правило с условием на пересылку от любого отправителя - определённому контакту (10000 + 1=10001) является более приоритетным, чем правило с условием на пересылку от определённой персоны - группе персон (5000 + 2500 = 7500).
Если количество баллов за отправителя-получателя у двух или более правил равно, то учитывается наличие в правиле условий на время и/или протокол. Если и в этом отношении правила равны, то отбираются несколько самых приоритетных правил с одинаковым приоритетом. Если суб-событию не соответствует ни одно правило, то выполняются действия по умолчанию (см. "Определение действий Системы по умолчанию").

5.8.1.4 Порядок применения действий согласно отобранным приоритетным правилам

Система назначает реакцию, выполняя действия из отобранных приоритетных правил, в следующем порядке:

1. Уведомляются все персоны, указанные в отобранных правилах
2. Назначаются все статусы, указанные в отобранных правилах
3. Событию присваивается наибольший уровень нарушения, указанный в отобранных правилах
4. Событие удаляется, если удаление указано хотя бы в одном правиле

5. Если хотя бы одно правило блокирует пересылку, пересылка блокируется
6. Событию присваиваются все теги, указанные в отобранных правилах

5.8.1.5 Пример:

Пусть в Системе заданы две политики:

Политика №1					
Каталог объектов защиты: Бухгалтерия					
Номер правила	Отправитель	Получатель	Время	**Протокол**	Реакция
1.1	Группа: Отдел продаж	Группа: Отдел Бухгалтерия	08:00 – 20:00	SMTP	Нарушение: Отсутствует
1.2	Иванов	Группа: Отдел Бухгалтерия		SMTP	Нарушение: Отсутствует
1.3	Иванов	<> Периметр: Компании			Нарушение: Средние
1.4	По умолчанию:				Нарушение: Высокое

Политика №2					
Каталог объектов защиты: Договорная					
Номер правила	Отправитель	Получатель	Время	**Протокол**	Реакция
2.1	Группа: Отдел продаж	<> Периметр: Компании	08:00 – 20:00	SMTP	Нарушение: Отсутствует
2.2	Иванов	<> Периметр: Компании		SMTP	Нарушение: Отсутствует
2.3	По умолчанию:				Нарушение: Отсутствует

Пусть Иванов входит в группу "*Отдел Продаж*". Петров входит в группу "*Отдел Бухгалтерия*". E-mail `sidorov@mail.com` находится за периметром компании.
Пусть есть событие:

Данные	Отправитель	Получатель	Время	**Протокол**
Группа объектов защиты: Бухгалтерия, Договорная	Иванов	Петров, sidorov@mail.com	19:00	SMTP

Это событие состоит из двух суб-событий, различающихся парами "отправитель-получатель": "Иванов->Петров" и "Иванов->sidorov@mail.com".

1. Проверка на соответствие политике №1.

200
Событие соответствует политике №1, так как в событии содержится *Группа объектов защиты - Бухгалтерия*.
Рассматривается суб-событие "Иванов->Петров":

Отправитель	Получатель	Время	**Протокол**
Иванов	Петров	19:00	SMTP

Этому суб-событию соответствует два суб-правила: №1.1 и 1.2. Из них более приоритетным является суб-правило №1.2. Следовательно, отбирается правило №1.2
Рассматривается суб-событие "Иванов->sidorov@mail.com":

Отправитель	Получатель	Время	**Протокол**
Иванов	sidorov@mail.com	19:00	SMTP

Этому суб-событию соответствует только суб-правило №1.3. Следовательно, отбирается правило №1.3

2. Проверка на соответствие политике №2.

Событие соответствует политике №2, так как в событии содержится *Группа объектов защиты - Договорная*
Рассматривается суб-событие "Иванов->Петров":

Отправитель	Получатель	Время	**Протокол**
Иванов	Петров	19:00	SMTP

Этому суб-событию соответствует только суб-правило №2.3. Следовательно, отбирается правило №2.3
Рассматривается суб-событие "Иванов->sidorov@mail.com":

Отправитель	Получатель	Время	**Протокол**
Иванов	sidorov@mail.com	19:00	SMTP

Этому суб-событию соответствует два суб-правила: №2.1 и 2.2. Из них более приоритетным является суб-правило №1.2. Следовательно, отбирается правило №2.2

3. Применяются отобранные действия: №1.2, №1.3, № 2.3, №2.2

5.8.2 Предустановленные политики

В Системе предустановлены следующие политики:

- Политики защиты конфиденциальных данных
- Политика контроля персон
- Политика, регулирующая передачу данных, защищенных паролем
- Политика, контроллирующая посещение веб-ресурсов сотрудниками компании

Примечание.

При удалении схемы БД (см. "*Infowatch Traffic Monitor. Руководство по установке*", статья "Удаление схемы базы данных") из Системы также удаляются политики, в том числе предустановленные.

Для повторного распространения предустановленных политик выполните следующие действия:

1. Создайте файл **/opt/iw/tm5/www/backend/protected/runtime/first_run** от имени пользователя **iwtm**;
2. Перезапустите процесс **iw_kicker**:
   ```
   service iwtm restart kicker
   ```

Остальные политики требуется создать повторно (см. "Создание политики защиты данных" и "Создание политики контроля персон").

5.8.2.1 Политики защиты конфиденциальных данных

По умолчанию в Системе создается по одной политике защиты данных для каждого предустановленного каталога объектов защиты (список предустановленных каталогов приведен в статье "Раздел "Объекты защиты"):

Предустановленные политики имеют следующие значения атрибутов:

Атрибут	**Значение**
Название политики	<Название каталога объектов защиты>
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Каталог <Название каталога объектов защиты>

где <Название каталога объектов защиты> - название того каталога, для которого создается политика.

Каждая политика содержит следующие правила:

Правила передачи

1. *Правило, регулирующее передачу конфиденциальных данных за периметр компании*.
   Если персона передает трафик любого типа за периметр компании в любой из дней недели,
   То Система выполнит следующие действия:
   - установит значение *Разрешено* атрибуту события *Вердикт*;
   - установит значение *Высокий* атрибуту события *Уровень нарушения*;
   - установит значение *Под наблюдением* атрибуту персоны-отправителя *Статус*.
2. *Правило, регулирующее передачу конфиденциальных данных руководством компании*.
   Если персон из группы VIP передает трафик любого типа любому получателю в любой из дней недели,
   То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Отсутствует* атрибуту события *Уровень нарушения*;
- установит событию тег *VIP*.

Правила копирования

Правило, регулирующее копирование конфиденциальной информации на съемные устройства.

Если персона копирует конфиденциальные данные на съемное устройство в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Высокий* атрибуту события *Уровень нарушения*;
- установит значение *Под наблюдением* атрибуту персоны-отправителя *Статус.*

5.8.2.2 Политика контроля персон

По умолчанию в Системе установлена политика контроля персон, имеющая следующие значения атрибутов:

Атрибут	Значение
Название политики	Персоны под наблюдением
Статус	Активная
Период действия	Не ограничен
Статусы	Под наблюдением

5.8.2.2.1 Правила политики

Правило, регулирующее передачу данных персоной, имеющей статус Под наблюдением.

Если персона, имеющая статус *Под наблюдением*, передает трафик любого типа любому получателю,
То Система установит значение *Поместить на карантин* атрибуту события *Вердикт*.

5.8.2.3 Политика, регулирующая передачу данных, защищенных паролем

По умолчанию в Системе установлена политика, регулирующая передачу данных, защищенных паролем.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Название политики	Данные, защищенные паролем
Статус	Активная
Период действия	Не ограничен

Атрибут	Значение
Защищаемые данные	Зашифрованные файлы всех файловых форматов

5.8.2.3.1 Правила политики

Правило, регулирующее передачу данных, защищенных паролем, за периметр компании.

Если персона передает трафик любого типа за периметр компании в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Высокий* атрибуту события *Уровень нарушения*;
- установит событию тег *На рассмотрение*.

5.8.2.4 Политики, контроллирующие посещение веб-ресурсов

По умолчанию в Системе установлены следующие политики защиты данных, контроллирующие посещение веб-ресурсов сотрудниками компании:

- Нецелевое использование ресурсов
- Нелояльные сотрудники
- Скрытые действия сотрудников
- Подозрительная активность

5.8.2.4.1 Нецелевое использование ресурсов

По умолчанию в Системе установлена политика, контроллирующая посещение развлекательных ресурсов сотрудниками компании.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Нецелевое использование ресурсов
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

5.8.2.4.1.1 ПРАВИЛА ПОЛИТИКИ

Правило передачи, контроллирующее отправку запросов на развлекательные ресурсы.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Медиа", "Блоги", "Развлечения", "Социальные сети" (подробнее см. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Низкий* атрибуту события *Уровень нарушения.*

5.8.2.4.2 Нелояльные сотрудники

По умолчанию в Системе установлена политика, предназначенная для отслеживания действий нелояльных сотрудников.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Нелояльные сотрудники
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

5.8.2.4.2.1 ПРАВИЛА ПОЛИТИКИ

Правило передачи, контроллирующее отправку запросов на сайты, связанные с поиском работы.

Если персона отправляет запрос на веб-ресурс, входящий в группу "Поиск работы" (подробнее см. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Средний* атрибуту события *Уровень нарушения.*

5.8.2.4.3 Скрытие действий сотрудников

По умолчанию в Системе установлена политика, позволяющая отслеживать скрытие сотрудниками своих действий и попытки обойти ограничения доступа к веб-ресурсам.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Скрытие действий сотрудников
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

5.8.2.4.3.1 ПРАВИЛА ПОЛИТИКИ

Правило передачи, контроллирующее отправку запросов на веб-анонимайзеры.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Анонимайзеры" (подробнее см. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Средний* атрибуту события *Уровень нарушения.*

5.8.2.4.4 Подозрительная активность

По умолчанию в Системе установлена политика, контроллирующая подозрительную активность сотрудников в интернете.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Подозрительная активность
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

5.8.2.4.4.1 ПРАВИЛА ПОЛИТИКИ

Правило передачи, контроллирующее отправку запросов на потенциально опасные ресурсы.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Потенциально опасные ресурсы", "Сайты агрессивной направленности", "Тематика для взрослых" (подробнее см. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Высокий* атрибуту события *Уровень нарушения;*
- установит событию тег *На рассмотрение*.

5.8.3 Создание политики защиты данных

Цель:
Создать политику, определяющую реакцию Системы на действия с данными.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области нажмите  и в раскрывающемся списке выберите **Политика защиты данных**.

3. Новая политика будет добавлена в группу **Политики защиты данных**, а в правой части рабочей области отобразится форма добавления политики.
4. Чтобы добавить в политику защищаемые данные, нажмите кнопку **Выбрать**.
   Если защищаемые данные не выбраны, будет создана политика на любые данные.
5. В открывшемся окне установите флажки напротив элементов, которые Вы хотите добавить, и нажмите **Добавить**. В качестве защищаемых данных могут выступать объекты защиты, их каталоги, а также файловые форматы.

> **Важно!**
>
> Если для политики указаны защищаемые данные нескольких типов, то для срабатывания правил политики (см. "Правила и форма их просмотра") необходимо, чтобы для события были обнаружены хотя бы по одному объекту каждого из указанных типов.
>
> Например, если в качестве защищаемых данных указаны каталог объектов защиты и несколько файловых форматов, то для срабатывания политики необходимо, чтобы в перехваченных данных содержался как минимум один объект защиты из указанного каталога и хотя бы один из указанных файловых форматов.

6. В правой части рабочей области заполните необходимые поля (см. "Политики и форма их просмотра") и нажмите **Сохранить**.

Пример 1:
Если требуется, чтобы Система реагировала на действия с данными, входящими в объект защиты *Гостайна*:
Офицер безопасности добавляет политику защиты данных и указывает в качестве защищаемых данных объект защиты *Гостайна*.

Пример 2:
Если требуется, чтобы Система реагировала на отправку любых данных на указанный ресурс:

Офицер безопасности добавляет политику защиты данных, указывает тип ресурса и уровень нарушения и не добавляет объекты исследования.

Дополнительные сведения:

- Редактирование политики описано в статье "Редактирование политики".
- Удаление политики происходит в результате нажатия кнопки , расположенной в правом верхнем углу плитки политики, и подтверждения удаления в открывшемся окне.

5.8.4 Создание политики контроля персон

Цель:
Создать политику, определяющую реакцию Системы на действия определенных персон.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области нажмите и в раскрывающемся списке выберите **Политика контроля персон**.

3. В открывшемся окне установите флажки напротив элементов, которые Вы хотите добавить, и нажмите **Создать**. В качестве объектов исследования могут выступать:
    - отдельные персоны (сотрудники или рабочие станции);
    - группы персон и рабочих станций;
    - персоны и рабочие станции, объединенные одним статусом.

> **Примечание.**
>
> Политика сработает при обнаружении хотя бы одного объекта из каждой группы.

4. Новая политика будет добавлена в группу **Политики контроля персон**, а в правой части рабочей области отобразится форма просмотра политики.
5. На форме просмотра политики заполните необходимые поля (см. "Политики и форма их просмотра") и нажмите **Сохранить**.

Вы также можете добавить политику для выбранной персоны, рабочей станции или группы непосредственно из раздела **Персоны**.
Для этого:

1. Перейдите в раздел **Персоны**.
2. Выделите нужную персону, рабочую станцию или группу.
3. На панели инструментов в правой части рабочей области нажмите и в раскрывающемся списке выберите **Создать политику**.

Пример:
Если требуется осуществлять контроль персоны *Иванов* (подразумевается, что персона Иванов уже создана в разделе **Персоны**) таким образом, чтобы объекту перехвата с уровнем нарушения *Высокий*, отправителем которого является данная персона, назначался вердикт *Разрешить*, при этом персоне присваивался статус *Под наблюдением*, и на почтовый ящик *example@company.com* отправлялось уведомление об инциденте:

Офицер безопасности переходит в раздел **Политики** и создает политику контроля персон с названием *Иванов*.

Далее Офицер безопасности создает правило для политики *Иванов*, при этом атрибутам должны быть присвоены следующие значения:

- атрибуту **Перехватывать с уровнем нарушения** - значение *Высокий*;
- атрибуту **Отправить уведомление** - значение *example@company.com* (подробнее см. "Отправка уведомления о сработавшем правиле");
- атрибуту **Назначить событию вердикт** - значение *Разрешить*;
- атрибуту **Назначить отправителю статус** - значение *Под наблюдением*.

Дополнительные сведения:

- Редактирование политики описано в статье "Редактирование политики".
- Удаление политики происходит в результате нажатия кнопки , расположенной в правом верхнем углу плитки политики, и подтверждения удаления в открывшемся окне.

5.8.5 Редактирование политики

Цель:
Изменить атрибуты созданной политики.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В правой части рабочей области заполните необходимые поля (см. "Политики и форма их просмотра").
4. Чтобы изменить список защищаемых данных или контролируемых персон, в блоке **Защищаемые данные** (для политик защиты данных) или **Контролируемые персоны** (для политик контроля персон) нажмите **Выбрать** и отредактируйте список, после чего нажмите **Сохранить**.
5. После внесения всех необходимых изменений на форме просмотра политики нажмите **Сохранить**.

5.8.6 Создание правил

Справочная информация:
Для каждой **политики защиты данных** вы можете настроить одно или несколько правил:

- Передачи объекта;
- Копирования объекта;
- Хранения объекта;
- Буфера обмена данных.

Если политика срабатывает на объекте перехвата, возможны следующие варианты, в зависимости от количества сработавших правил:

- Если срабатывает одно правило, Система выполняет действия, указанные для этого правила.
- Если срабатывают несколько правил, и
    - действия сработавших правил противоречат друг другу - Система выбирает из противоречащих действий самое приоритетное и выполняет его (о порядке выбора приоритетов см. "Общие сведения о политиках");
    - действия сработавших правил не противоречат друг другу - Система выполняет все действия, не противоречащие другим.
- Если ни одно правило не срабатывает, либо правила не заданы, Система выполняет действия, заданные для этого правила по умолчанию (см. "Определение действий Системы по умолчанию").

Для каждой **политики контроля персон** вы можете настроить правила перехвата событий с указанным уровнем нарушения. Вы также можете связать правило с имеющими в Системе политиками защиты данных.

Примечание:

Если на объекте перехвата срабатывают несколько политик, каждая из которых имеет правила, Система выбирает из противоречащих действий наиболее приоритетное и выполняет его (о порядке выбора приоритетов см. "Общие сведения о политиках"); действия, не противоречащие другим, выполняются в полном объеме.

Цель:
Определить, какие действия с защищаемыми данными необходимо произвести, чтобы вызвать реакцию Системы, и как Система должна отреагировать на эти действия.

Решение:

1. Перейдите в раздел **Политики**.
2. Добавьте правило одним из следующих способов:
   - Щелчком левой кнопки мыши выделите целевую политику защиты данных, в левой части плитки политики выберите вкладку (**Передача**, **Копирование**, **Хранение** или **Буфер обмена**), в зависимости от требуемой задачи, и нажмите **Добавить правило**.
   - Щелчком левой кнопки мыши выделите целевую политику защиты данных, а затем в правой части рабочей области, нажмите **Добавить правило**, и в выпадающем списке выберите требуемое правило.
3. Настройте правило, используя форму в правой части рабочей области (см. "Правила и форма их просмотра").
4. В блоке **Действия при срабатывании правила** на форме просмотра правила укажите, какие действия должна выполнить Система в случае срабатывания правила.

Пример:

Если требуется, чтобы в случае передачи файлов, составляющих объект защиты *Строго конфиденциальная информация*, по субботам и воскресеньям, Система присваивала событию тег *Отправка конфиденциальной информации в выходные* и назначала уровень нарушения *Средний*: Офицер безопасности выполняет следующие действия:

1. создает тег *Отправка конфиденциальной информации в выходные* (см. "Работа с тегами");
2. создает политику защиты данных для объекта защиты *Строго конфиденциальная информация* (см. "Создание политики защиты данных");
3. создает правило передачи, присвоив атрибуту **Дни недели действия** значения *Суббота* и *Воскресенье;*
4. в блоке **Действия при срабатывании правила** присваивает атрибутам следующие значения:
   - атрибуту **Назначить событию уровень нарушения** - значение *Средний*;
   - атрибуту **Теги** - значение *Отправка конфиденциальной информации в выходные*.

Дополнительные сведения:

- Редактирование правил описано в статье "Редактирование правил".
- Удаление правила происходит после нажатия кнопки ×, расположенной в правом верхнем углу плитки правила, и подтверждения удаления в открывшемся окне.

5.8.7 Редактирование правил

Цель:
Отредактировать ранее созданное правило.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политики выберите целевую группу правил (вкладки **Передачи**, **Копирования, Хранения** или **Буфера обмена** для политики защиты данных или вкладка **Правила** для политики контроля персон).
4. В плитке политике отобразится список правил выбранной группы. Щелчком левой кнопки мыши выделите нужное правило в списке.
5. В правой части рабочей области откроется форма редактирования правила. Измените необходимые поля (см. "Правила и форма их просмотра") и нажмите **Сохранить**.

5.8.8 Определение действий Системы в случае нарушения правил

Справочная информация:
Для каждой политики вы можете указать действия, выполняемые Системой в случае нарушения правил.

Доступные действия определяются типом правила:

Действие	**Политики защиты данных**			**Политики контроля персон**
	Правило передачи	**Правило копирования**	**Правило хранения**	**Правило контроля персон**
Отправить уведомление пользователям	Доступно	Доступно	Доступно	Доступно
Уведомить нарушителя	Доступно только для типа событий "Электронная почта"	Не доступно	Не доступно	Не доступно
Назначить событию вердикт	Доступно	Не доступно	Не доступно	Доступно
Назначить событию уровень нарушения	Доступно	Доступно	Доступно	Доступно
Назначить событию теги	Доступно	Доступно	Доступно	Доступно
Назначить отправителю статус	Доступно	Доступно	Доступно	Доступно
Удалить событие	Доступно	Доступно	Доступно	Доступно

Подробное описание действий:

Действие	Описание
Отправить уведомление пользователям	Указанным пользователям Консоли будет отправлено уведомление по электронной почте. В списке можно указать пользователей или их email-адреса.
Уведомить нарушителя	Отправителю перехваченного электронного письма будет выслано уведомление
Назначить событию вердикт	Событию будет назначен вердикт - предварительное решение Системы о возможном нарушении политики безопасности. Возможные значения: • **Разрешить** - объект не является потенциальным нарушением и может быть доставлен получателям. • **Заблокировать** - объект является потенциальным нарушением. В режиме "Блокировка" доставка такого объекта блокируется. • **Поместить на карантин** - требуется решения пользователя, является ли объект нарушением. В режиме "Блокировка" доставка такого объекта откладывается до вынесения решения пользователем. В зависимости от решения пользователя значение вердикта изменится либо на **Разрешено** (в этом случае выполняется доставка), либо на **Заблокировано** (подробнее см. "Вынесение решения по объекту"). Досылка сообщений возможна только для SMTP-писем при работе Системы "в разрыв" - см. документ "*Infowatch Traffic Monitor. Руководство по установке и настройке*".
Назначить событию уровень нарушения	Событию будет назначен уровень нарушения. Возможные значения: **Высокий**, **Средний**, **Низкий**, **Отсутствует**.
Назначить событию теги	Событию будут назначены указанные теги, например, **На рассмотрение**. Подробнее см. "Теги".
Назначить отправителю статус	Нарушителям политики безопасности будет присвоен указанный статус, например, **Под наблюдением**. Подробнее см. "Статусы".
Удалить событие	Событие не будет сохранено в базу данных, а также не будут выполнены действия, указанные в правиле.

Цель:

Определить, как должна отреагировать Система в случае нарушения правил политики.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите нужную политику.
3. В плитке политики нажмите на ссылку с требуемой группой правил (**Передачи**, **Копирования** или **Хранения** для политики защиты данных или **Правила** для политики контроля персон).
4. Щелчком левой кнопки мыши выделите нужное правило из списка правил или нажмите **Добавить правило** для создания нового правила (см. "Создание правил").
5. В правой части рабочей области, в блоке **Действия**, укажите, какие действие должна выполнить Система в случае срабатывания правила.
6. Нажмите **Сохранить**.

См. также:

- "Редактирование правил" - об изменении созданных правил

5.8.9 Определение действий Системы по умолчанию

Справочная информация:
Если после применения политики остаются суб-события, которым не соответствует ни одно правило, Система выполняет действия по умолчанию (о разбиении событий на суб-события см. "Общие сведения о политиках"). Действия по умолчанию определяются пользователем.

> **Примечание.**
>
> Если действие по умолчанию не заданы и не сработало ни одно из правил, то политика защиты данных также не сработает на объекте перехвата.

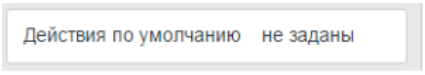
Цель:

Определить, как должна отреагировать Система при наличии в событии суб-события, которому не соответствует ни одно правило политики.

> **Примечание.**
>
> Возможность указать действия по умолчанию предусмотрена только для политики защиты данных.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политики выберите целевую вкладку (**Передача**, **Копирование** или **Хранение**), в зависимости от требуемой задачи, и щелчком левой кнопкой мыши выделите нижнюю часть плитки:



4. В правой части рабочей области измените необходимые поля в единственном блоке **Действия** (см. "Правила и форма их просмотра") и нажмите **Сохранить**.

Дополнительная информация:

Для типов события Web-сообщение и Web-почта может возникать ситуация, когда происходит ложное срабатывание правила по умолчанию. Такая ситуация может возникнуть, если:

В Системе создано правило, регулирующее передачу данных от персоны А к персоне В. Если персона А отправляет данные персоне В через Web-сайт, в Системе создается событие, которое разбивается на два суб-события:

Отправитель	Получатель	Протокол

Отправитель	Получатель	Протокол
Персона A	Персона B	HTTP
Персона A	Домен Web-сайта	HTTP

Так как маршрут **Персона A**->**Домен Web-сайта** не описан в правилах политики, выполняются действия по умолчанию.

Чтобы избежать ложного срабатывания правила по умолчанию для типов события Web-сообщение и Web-почта, вы можете:

- добавить в правило передачи домен Web-сайта или список Web-сайтов, через которые может осуществляться передача данных;
- не указывать действия по умолчанию.

Пример:

Требуется, чтобы в случае копирования файлов, составляющих объект защиты *Гостайна*, при отсутствии сработавших правил копирования Система по умолчанию присваивала карточке копирующей персоны статус *Под наблюдени*ем:
В этом случае офицер безопасности выполняет следующие действия:

1. создает политику защиты данных для объекта защиты *Гостайна* (см. "Создание политики"),
2. переходит к заданию действий политики по умолчанию,
3. в единственном разделе **Действия** присваивает атрибуту **Назначить отправителю статус** значение *Под наблюдением.*

5.8.10 Фильтрация списка политик

Цель:
Отфильтровать список политик в случае большого числа политик в списке.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области нажмите **Фильтр**.
3. Укажите критерии фильтрации в одном из полей или в обоих полях:
    - **Фильтровать по названиям политик** - начните вводить текст и выберите название требуемой политики (возможно выбрать несколько политик, повторяя данное действие);
    - **Фильтровать по объектам исследования** - начните вводить текст и выберите название требуемого объекта (возможно выбрать несколько объектов, повторяя данное действие).
4. Нажмите **Применить**.

5.8.11 Отправка уведомлений о сработавшем правиле

Цель:
Настроить автоматическое уведомление пользователей Системы о сработавшем правиле.

Важно!

Для отправки уведомлений можно использовать только email-адрес. При выборе из существующих контактов пользуйтесь записями только тех пользователей, у которых указан email-адрес.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политике выберите требуемую вкладку (**Передача**, **Копирование** или **Хранение**) и левой кнопкой мыши выделите целевое правило из списка правил.
4. В плитке политики отобразится список правил выбранной группы. Щелчком левой кнопки мыши выделите нужное правило в списке.
5. В правой части рабочей области в поле **Отправить уведомление** укажите контакт пользователя Консоли управления. Для этого начните вводить контактные данные и выберите из раскрывающегося списка необходимую запись.

Примечание.

Если после создания правила пользователь или его e-mail будут удалены из Системы (о работе с учетными записями пользователей см. *"Руководство администратора"*, раздел "Пользователи"), то уведомление данному пользователю отправлено не будет.

Пример:

Если требуется, чтобы при копировании конфиденциальных данных (объект защиты - *Коммерческая_тайна*) на съемный носитель по субботам и воскресеньям Система назначала объекту перехвата вердикт *Разрешить*, при этом персоне, выполняющей копирование, в Системе присваивался статус *Под наблюдением*, и на почтовый ящик *example@company.com* отправлялось уведомление об инциденте:
Офицер безопасности создает политику защиты данных для объекта защиты *Коммерческая_тайна*.
Далее офицер безопасности создает правило копирования для созданной политики и присваивает следующие значения атрибутам:

- атрибуту **Дни недели действия правила** - значение *суббота* и *воскресенье*;
- атрибуту **Устройства** - значение *Съемные устройства* или *Принтеры или съемные устройства*;
- атрибуту **Отправить уведомление** - значение *example@company.com*;
- атрибуту **Назначить вердикт** - значение *Разрешить.*

5.9 Работа с отчетами

Для чего требуется работа с отчетами:

В отличие от краткой статистической информации, представленной в разделе "Сводка", отчеты позволяют выполнить более гибкую настройку параметров статистики и наглядно продемонстрировать результаты работы Системы за указанный период времени.

Работа с отчетами состоит из следующих действий:

Действие	Описание
Создание папки с отчетами	Создание папки, в которой будут храниться отчеты
Создание отчета	Формирование отчета со статистической информацией
Работа с виджетами	Указание параметров поиска и способа графического отображения данных в отчете
Работа с готовыми отчетами	Просмотр истории выполнения отчета с возможностью удалить ненужные версии отчета или сохранить данные отчета в файл

См. также:

- "Раздел Отчеты" - о разделе, в котором ведется работа с отчетами

5.9.1 Создание папки с отчетами

Цель:
Создать папку, в которой будут сгруппированы отчеты, объединенные общей тематикой.

Решение:

1. Перейдите в раздел **Отчеты**.
2. На панели инструментов в левой части рабочей области нажмите  и в раскрывающемся списке выберите **Создать папку**.
3. В открывшейся окне создания отчета укажите название папки и параметры доступа (подробнее см. "Форма создания папки с отчетами").
4. Нажмите **Сохранить папку**.

Вы также можете скопировать ранее созданную папку и содержащиеся в ней отчеты. Для этого:

1. Выделите нужную папку в списке с помощью мыши.
2. На панели инструментов в левой части рабочей области нажмите  **Копировать**.
3. Копия будет добавлена в структуру папок на том же уровне, что и копируемая папка.

Вы можете изменить расположение папки, используя перетаскивание. Для этого выделите в списке нужную папку и, удерживая левую клавишу мыши зажатой, переместите ее в требуемое место, после чего отпустите зажатую клавишу мыши.

Дополнительные сведения:

Редактирование и удаление папки выполняются следующим способом:

- редактирование папки выполняется стандартным способом (см. "Редактирование элемента");
- удаление папки выполняется стандартным способом (см. "Удаление элемента").

5.9.2 Создание отчета

Цель:
Создать отчет, содержащий статистические данные по объектам перехвата.

Решение:

1. Перейдите в раздел **Отчеты**.
2. В левой части рабочей области выберите папку, в которой требуется создать отчет, либо создайте новую папку (подробнее см. "Создание папки с отчетами").
3. На панели инструментов нажмите  и в раскрывающемся списке выберите **Создать отчет**.
4. В открывшейся форме создания отчета укажите требуемые параметры (подробнее см. "Форма создания отчета").
5. Нажмите **Добавить виджет**.
6. В открывшемся окне **Создание виджета** укажите параметры виджета (подробнее см. "Работа с виджетами отчетов").
7. Нажмите:
    a. **Сохранить** - чтобы сохранить отчет.
    b. **Сохранить и выполнить** - чтобы сохранить и выполнить отчет.

Вы также можете скопировать ранее созданный отчет. Для этого:

1. Выделите нужный отчет в списке с помощью мыши.
2. На панели инструментов в левой части рабочей области нажмите  **Копировать** (либо нажмите на кнопку  в правой части рабочей области и в раскрывающемся списке выберите **Скопировать**).
3. Копия будет добавлена в структуру отчетов на том же уровне, что и копируемый отчет.

Вы можете изменить расположение отчета, переместив его с помощью мыши. Для этого выделите в списке нужный отчет и, удерживая левую клавишу мыши зажатой, перетащите его в требуемое место, после чего отпустите зажатую клавишу.

Важно!

При перемещении отчета к нему будут применены параметры доступа, указанные для папки, в которую вы перемещаете отчет.

Дополнительные сведения:

Редактирование и удаление отчета выполняются стандартным способом:

- Редактирование отчета выполняется стандартным способом (см. "Редактирование элемента"). Помимо кнопки , расположенной на панели инструментов, вы можете использовать кнопку **Редактировать** в правой части рабочей области;
- Удаление отчета выполняется стандартным способом (см. "Удаление элемента"). Помимо кнопки , расположенной на панели инструментов, вы можете использовать удалить отчет, нажав на кнопку  в правой части рабочей области и выбрав команду **Удалить**.

5.9.3 Работа с виджетами отчетов

Работа с виджетами состоит из следующих действий:

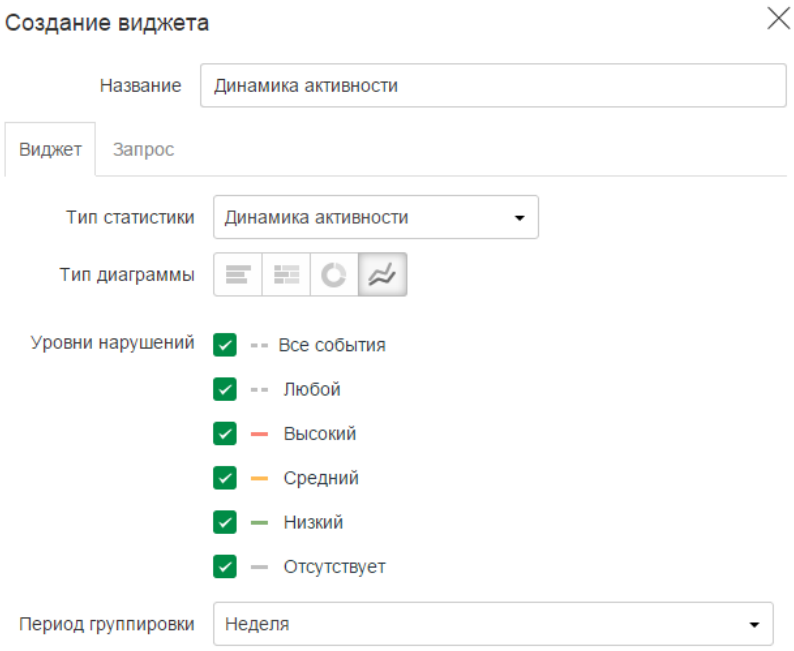
Действие	Описание
Создание и настройка виджета	Чтобы указать способ отображения статистических данных и условия фильтрации, требуется создать и настроить виджет
Редактирование виджета	Для редактирования виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите  и в раскрывающемся списке выберите **Редактировать**.
Дублирование виджета	Для дублирования виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите  и в раскрывающемся списке выберите **Дублировать**. В списке отчетов в левой части рабочей области выберите отчет, в который требуется дублировать виджет.
Удаление виджета	Для удаления виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите  и в раскрывающемся списке выберите **Удалить**.

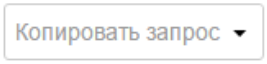
5.9.3.1 Создание и настройка виджета

Цель:
Создать виджет для выбранного отчета и настроить его параметры.

Решение:

1. Перейдите в раздел **Отчеты**.
2. Выберите требуемый отчет и перейдите в режим редактирования либо создайте новый отчет (подробнее см. "Создание отчета").
3. В правой части рабочей области нажмите кнопку **Добавить виджет**. Откроется окно **Создание виджета**.



4. Заполните требуемые поля:
    a. В поле **Название** введите название виджета.
    b. На вкладке **Виджет** выберите тип статистики. Остальные настройки (тип диаграммы, число записей, период группировки и т.д.) доступны в зависимости от выбранного типа статистики (подробнее о типах статистики см. статью "Виджеты").
    c. На вкладке **Запрос** укажите параметры, на основе которых будет выполняться фильтрация событий (подробнее о доступных параметрах см. статью "Запросы"). Чтобы скопировать параметры из запроса, созданного в разделе События, нажмите 

и в раскрывающемся списке выберите требуемый запрос.
5. Нажмите **Сохранить виджет**.

5.9.4 Работа с готовыми отчетами

Работа с готовыми отчетами состоит из следующих действий:

- просмотр истории выполнения отчета;
- просмотр выбранной версии отчета;
- удаление выбранных записей;
- выгрузка отчета в файл.

Для просмотра данных о выполнении отчета:

1. Перейдите в раздел **Отчеты**.

2. В правой части рабочей области нажмите кнопку  и в раскрывающемся списке выберите **История выполнения отчета**. В открывшемся диалоговом окне вы можете просмотреть данные о выполнении отчета (подробнее см. "История выполнения отчета").
3. Чтобы добавить комментарий к выбранной версии отчета, дважды щелкните левой клавишей мыши в поле **Комментарий** напротив выбранной версии и введите текст.

Для просмотра и редактирования выбранной версии отчета:

1. Чтобы открыть отчет за определенную дату, щелкните по требуемой дате выполнения левой клавишей мыши. Откроется список виджетов, отображающих результат выполнения отчета за выбранную дату.
2. Если вы хотите перейти к разделу "События" и просмотреть события, отображаемые на виджете, нажмите на кнопку в верхнем правом углу выбранного виджета и в раскрывающемся списке выберите **Перейти в события**.

Для удаления выбранных версий отчета:

1. Выберите версии отчета, которые вы хотите удалить. Для этого установите флажки в нужных строках. Чтобы выбрать все строки сразу, установите флажок в заголовке.
2. Нажмите **Удалить**.

Для выгрузки отчета:

1. Выберите версии отчета, которые Вы хотите сохранить в файл. Для этого установите флажки в нужных строках. Чтобы выбрать все строки сразу, установите флажок в поле заголовка.
2. Нажмите **Выгрузить** и в раскрывающемся списке укажите требуемый формат сохранения. Вы можете сохранить отчет в одном из следующих форматов: Excel 2007, Excel 2003, HTML или PDF. Файл в указанном формате будет сохранен на ваш компьютер.

> **Примечание:**
>
> Чтобы выгрузить текущую версию отчета, в правом верхнем углу рабочей области нажмите  и в раскрывающемся списке под заголовком **Выгрузка отчета** выберите формат, в котором требуется сохранить выгрузку. Файл в указанном формате будет сохранен на ваш компьютер.

6 ЛИЦЕНЗИОННАЯ ИНФОРМАЦИЯ

Лицензионная информация для Системы приведена в следующих разделах:

- Пользовательское лицензионное соглашение
- Лицензии третьих сторон

6.1 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями лицензионного соглашения перед началом работы с программным обеспечением.
Нажатие Вами кнопки подтверждения согласия в окне с текстом лицензионного соглашения при установке программного обеспечения или использование устанавливаемого программного обеспечения означает Ваше безоговорочное согласие с условиями настоящего лицензионного соглашения. Если Вы не согласны с условиями настоящего лицензионного соглашения, Вы должны прервать установку и/или использование программного обеспечения.

6.1.1 Лицензионное соглашение

Настоящее пользовательское лицензионное соглашение (далее – Соглашение) является Договором присоединения между АО «ИнфоВотч» (далее – Правообладатель) и Вами, физическим или юридическим лицом (далее – Пользователь), правомерно владеющим экземпляром программного комплекса InfoWatch Traffic Monitor – (далее – Система).
Система предназначена для мониторинга, фильтрации и предотвращения утечки данных, передаваемых за пределы компании по электронной почте, через Интернет и интернет-пейджеры, а также сетевой и локальной печати. Система также позволяет контролировать доступ к портам персональных компьютеров и осуществлять мониторинг данных, копируемых на сменные устройства.

6.1.1.1 1. Определения

1.1. ПО – обозначает, как вместе, так и по отдельности, Систему, сопроводительные материалы, Документация к Системе, дополнительно заказанные обновления Системы, правообладателем которых является АО «ИнфоВотч».
1.2. Компьютер – оборудование, для работы на котором предназначено ПО, на которое устанавливается Система и/или на котором используется Система.
1.3. Пользователь (Вы) – лицо, которое устанавливает или использует ПО от своего лица или правомерно владеет копией ПО. Если ПО было загружено или приобретено от имени юридического лица, то под термином Пользователь (Вы) далее подразумевается юридическое лицо, для которого ПО было загружено или приобретено и которое поручило отдельному физическому лицу принять данное соглашение от своего лица.

1.4. Партнеры – организации, осуществляющие распространение ПО на основании договора с Правообладателем.
1.5. Документация к Системе – сопроводительные печатные и иные материалы, Руководство Пользователя, Руководство Администратора, справочник, файл справки и аналогичные им сопроводительные печатные и электронные документы в отношении Системы, правообладателем которых является АО «ИнфоВотч».

6.1.1.2 2. Предоставление лицензии

2.1. Правообладатель предоставляет Вам неисключительную лицензию на использование ПО в рамках функциональности, описанной в Документации к Системе, при условии соблюдения Вами всех технических требований, описанных в Документации к Системе, а также всех ограничений и условий использования Системы, указанных в настоящем Соглашении.
2.2. В случае если Вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, Вы имеете право использовать ПО только в целях ознакомления и только в течение одного ознакомительного периода, если не прописано иначе, начиная с даты начальной установки ПО. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.
2.3. Если Вы используете ПО разных версий или версии ПО для разных языков, если Вы получили ПО на нескольких носителях, если Вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее количество Ваших компьютеров, на которых установлены и/или используются все версии Системы, должно соответствовать количеству лицензий, полученных от Правообладателя в том случае, если условия лицензии не утверждают иное; каждая купленная лицензия дает Вам право установить и использовать Систему на таком количестве компьютеров и/или в отношении определенного количества лицензионных объектов, которое указано в п.2.2.
2.4. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.
2.5. Любая правомерная передача прав в отношении пользования ПО возможна только при условии присоединения к настоящему соглашению и с предварительного согласия Правообладателя или его уполномоченного Партнера. При этом, правопреемник Пользователя в отношении использования ПО становится законным правопреемником Пользователя в отношении использования ПО только при условии полного замещения Пользователя по настоящему соглашению.
2.6. Вы самостоятельно несете ответственность и обеспечиваете соблюдение применимого экспортного и импортного законодательства, а также применимых торговых санкций и эмбарго в отношении передачи прав и использования ПО.

6.1.1.3 3. Ограничения

3.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично, за исключением случаев, предусмотренных законодательством.
3.2. Запрещается передавать право на использование ПО третьим лицам за исключением случая, указанного в п. 2.6.
3.3. Запрещается передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения, за исключением случая, указанного в п.2.6 настоящего Соглашения. Лицензионный ключ являются конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности

установленного у Вас лицензионного ключа.
3.4. Запрещается сдавать ПО в аренду, прокат или во временное пользование, а так же разглашать результаты стендовых испытаний Системы.
3.5. Правообладатель имеет право заблокировать лицензионный ключ в случае нарушения Пользователем условий настоящего Соглашения.
3.6. При использовании Вами ПО, предназначенного для ознакомительных целей, Вы не имеете права передавать имеющийся у Вас экземпляр ПО третьим лицам.
3.7. За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.
3.8. Вы не вправе использовать ПО для любых целей или способом ограниченным или запрещенным применимым законодательством. Вы самостоятельно несете ответственность за неправомерное использование ПО.
3.9. В случае нарушения Вами какого-либо из условий данного Соглашения Правообладатель вправе прервать действие Соглашения на использование ПО в любое время без Вашего уведомления и без возмещения стоимости ПО или его части.

6.1.1.4 4. Ограниченная гарантия и отказ от предоставления гарантий

4.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Документации к Системе.
4.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.
4.3. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Документации к Системе, а также в случае нарушения Пользователем условий настоящего Соглашения.
4.4. ЗА ИСКЛЮЧЕНИЕМ УСТАНАВЛИВАЕМОЙ В НАСТОЯЩЕМ ПУНКТЕ ОГРАНИЧЕННОЙ ГАРАНТИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ. ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЫ СОГЛАШАЕТЕСЬ С ТЕМ, ЧТО ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ.

6.1.1.5 5. Ограничение ответственности

В МАКСИМАЛЬНОЙ СТЕПЕНИ, ДОПУСКАЕМОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО УБЫТКИ И/ИЛИ УЩЕРБ (В ТОМ ЧИСЛЕ УБЫТКИ В СВЯЗИ С НЕДОПОЛУЧЕННОЙ КОММЕРЧЕСКОЙ ПРИБЫЛЬЮ, ПРЕРЫВАНИЕМ ДЕЯТЕЛЬНОСТИ, УТРАТОЙ ИНФОРМАЦИИ ИЛИ ИНОЙ ИМУЩЕСТВЕННЫЙ УЩЕРБ), ВОЗНИКАЮЩИЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ БЫЛИ УВЕДОМЛЕНЫ О ВОЗМОЖНОМ ВОЗНИКНОВЕНИИ ТАКИХ УБЫТКОВ И/ИЛИ УЩЕРБА. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПРАВООБЛАДАТЕЛЯ И ЕГО ПАРТНЕРОВ ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ВАМИ ЗА

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. НАСТОЯЩИЕ ОГРАНИЧЕНИЯ НЕ МОГУТ БЫТЬ ИСКЛЮЧЕНЫ ИЛИ ОГРАНИЧЕНЫ В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ПРАВОМ.

6.1.1.6 6. Программные продукты

6.1. Технология третьих лиц, которая может быть целесообразна или необходима для использования в составе ПО определена в Документации к Системе. Такая технология лицензируется конечному пользователю на условиях лицензионного соглашения третьего лица, определенного в Документации к Системе. Такое лицензионное соглашение третьего лица дополняет положения настоящего Соглашения.
6.2. Входящие в состав Системы программные продукты лицензированы для ограниченного использования только в составе Системы. По истечении срока лицензионного использования ПО, пользователь обязан прекратить использование ПО и уничтожить все имеющиеся копии.

6.1.1.7 7. Открытое (свободное) программное обеспечение

Данный продукт может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду ("ПО с открытым исходным кодом"). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса Правообладателю или сопровождается с продуктом. Если какая-либо лицензия на ПО с открытым исходным кодом требует, чтобы Правообладатель предоставлял права на использование, копирование или модификацию ПО с открытым исходным кодом, выходящие за рамки прав, предоставляемых настоящим Соглашением, такие права имеют преимущественную силу над правами и ограничениями, оговоренными в настоящем Соглашении.

6.1.1.8 8. Права на интеллектуальную собственность

8.1. Вы соглашаетесь с тем, что ПО, документация, как и все другие объекты авторского права, а также системы, идеи и методы работы, другая информация, которая содержится в ПО, товарные знаки являются объектами интеллектуальной собственности Правообладателя или его Партнеров. Данное Соглашение не дает Вам никаких прав на использование объектов интеллектуальной собственности, включая товарные знаки и знаки обслуживания Правообладателя или его Партнеров, за исключением прав, предоставленных настоящим Соглашением.
8.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя или его соответствующих контрагентов.
8.3. Вы не можете удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

6.1.1.9 9. Контактная информация Правообладателя

АО «ИнфоВотч»
Тел./факс:+7(495)229-00-22
Департамент продаж: sales@infowatch.com
Служба технической поддержки: support@infowatch.com
Веб-сайт: www.infowatch.ru

6.2 Лицензии третьих сторон

При создании Системы были использованы разработки третьих сторон, распространяемые на условиях лицензии MIT (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

Также использовалось программное обеспечение:

- распространяемое на условиях лицензий BSD (http://www.opensource.org/licenses/bsd-license.php):
    - - Stringencoders – http://code.google.com/p/stringencoders/
- распространяемое на условиях GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
    - - Pdftotext – http://www.foolabs.com/xpdf/
    - - Tnef – http://sourceforge.net/projects/tnef/
    - - Unzip – http://www.info-zip.org/UnZip.html
    - - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
    - - libhtmltree.so – pauljlucas@mac.com

7 ГЛОССАРИЙ

Термин	Определение
"В разрыв"	Схема развертывания IW TM, при которой возможно блокирование исходящих из периметра почтовых сообщений с последующей досылкой. При этом сервер IW TM используется в качестве relay-сервера.
Active Directory	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
AJAX	Asynchronous Javascript and XML (асинхронный JavaScript и XML) - подход к построению интерактивных пользовательских интерфейсов веб-приложений, заключающийся в «фоновом» обмене данными браузера с веб-сервером
DeviceLock	Средство защиты информации от утечек (DLP), осуществляющее контроль и протоколирование доступа пользователей к устройствам, портам ввода-вывода и сетевым протоколам
DeviceLock Adapter	Перехватчик IW DM, обеспечивающий интеграцию с системой DeviceLock, выполняющей перехват теневых копий файлов, переносимых на съемные устройства. См. также: IW DM, Теневая копия файла, Перехватчик
Domino directory	IBM Lotus Domino Directory - это директория с информацией о пользователях, серверах и группах. Domino Directory - это инструмент, используемый для администрирования системы Domino.
FTP	File Transfer Protocol (протокол передачи файлов) - сетевой протокол, предназначенный для передачи файлов по TCP-сетям
GTalk	Google Talk — программное обеспечения для мгновенного обмена сообщениями, разработанное компанией Google
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста) - протокол прикладного уровня передачи данных в виде текстовых сообщений. См. также: HTTPS, HTTP(S) Monitor
HTTPS	HyperText Transfer Protocol Secure (защищенный протокол передачи гипертекста) - расширение протокола HTTP, поддерживающее шифрование. См. также: HTTP, HTTP(S) Monitor
HTTP-запрос	Запрос, удовлетворяющий требованиям протокола HTTP (POST-запрос, GET-запрос и т. д.). См. также: HTTP, Событие
ICAP	Internet Content Adaptation Protocol - протокол, позволяющий контролировать входящий и исходящий HTTP-трафик. Предоставляет возможность модификации содержимого HTTP-запросов.
ICQ	Служба мгновенного обмена сообщениями в сети Интернет. Использует протокол OSCAR.
ICQ-сообщение	Сообщение, передаваемое по протоколу ICQ-OSCAR. См. также: Событие

Термин	Определение
IMAP	Internet Message Access Protocol Version 4 (протокол доступа к электронной почте Интернета) - сетевой протокол для доступа к электронной почте.
InfoWatch Device Monitor	IW DM: программный комплекс, предназначенный для контроля доступа сотрудников к периферийным устройствам и сетевым ресурсам, мониторинга операций (копирование данных на съемные носители и сетевые хранилища, отправка данных на печать, сетевая активность, использование приложений, фото) и перехвата трафика систем мгновенного обмена сообщениями (Skype, Gtalk, Yahoo, Mail.ru Agent и Jabber) и т.п.
InfoWatch Traffic Monitor	IW TM: программный комплекс, предназначенный для осуществления контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, YMSG, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать.
IW Lync Adapter	Перехватчик событий обмена данными через сервера MS Lync, установленные в инфраструктуре компании.
Jabber	Система для быстрого обмена сообщениями и информацией о присутствии на основе открытого протокола XMPP
Lotus Adapter	Перехватчик, который устанавливается на почтовом сервере IBM Lotus для перенаправления писем для анализа при помощи IW TM. См. также: Перехватчик
Lotus Domino	Почтовый сервер компании IBM, сообщения которого перехватываются при помощи Lotus Adapter.
Mail.Ru Агент	Программа для быстрого обмена сообщениями через Интернет, поддерживающая возможности IP-телефонии, видеозвонки и отправку SMS
MAPI	Messaging Application Programming Interface - программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений
MMP	Протокол соединения Mail.Ru агента с общей сетью Mail.ru
MS Lync	Универсальный клиент Microsoft для общения и обмена информацией
POP3	Post Office Protocol Version 3 (протокол почтового отделения) - сетевой протокол, используемый для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению
POST-запрос	Метод запроса POST предназначен для запроса, при котором веб-сервер принимает данные, заключенные в тело сообщения, для хранения. Он часто используется для загрузки файла или представления заполненной веб-формы
Relay-сервер	Сервер, выполняющий получение/пересылку электронной почты.
Skype	Служба, обеспечивающая текстовую, голосовую и видеосвязь через Интернет
SMB	Server Message Block - сетевой протокол для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol (простой протокол передачи почты) - сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP

Термин	Определение
SMTP-письмо	Письмо, удовлетворяющее требованиям протокола SMTP. См. также: SMTP, Событие
SPAN	Switched Port Analyzer - технология зеркального копирования трафика с одного порта на другой
SPAN-копия	Разновидность транспортного режима Копия. Передача трафика в этом режиме осуществляется через коммутатор CISCO. Копия трафика передается для анализа на сервер Traffic Monitor. См. также: SPAN
SSL	Secure Sockets Layer (уровень защищённых сокетов) - криптографический сетевой протокол, обеспечивающий защищенный обмен данными
WhatsApp	Мессенджер для смартфонов, позволяющий пересылать текстовые сообщения, изображения, аудио- и видео-файлы; а также используемый в нем протокол.
XMPP	Extensible Messaging and Presence Protocol - сетевой протокол, обеспечивающий мгновенный обмен сообщениями и информацией о присутствии
Yahoo	Система для быстрого обмена сообщениями и информацией на основе открытого протокола YMSG
Администратор	Предустановленная роль и учетная запись консоли управления, имеющая права на управление другими учетными записями и их правами. Также Администратор - пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Роль пользователя, Офицер безопасности, Пользователь
Активная политика	Политика, действующий в конфигурации, загруженной на хост. См. также: Политика, Хост
Анализ события	Процедура обработки атрибутов, вложенных файлов и текста перехваченных событий и назначения событию дополнительных атрибутов. См. также: Политика, Атрибуты события, Событие
Атрибуты события	Структурированные данные, извлеченные из перехваченных событий и назначенные по результатам их обработки. См. также: Событие, Политика, Вердикт, Решение, Транспортный режим
Аудит	Контроль действий, выполняемых пользователями Консоли управления: создание и управление схемой безопасности, администрирование Системы. См. также: Журнал аудита, Учетные записи Консоли управления
База данных	Совокупность данных, хранимых в соответствии с используемой схемой данных. Хранит всю информацию, необходимую для работы Системы.
Бланки	Технология поиска заполненных бланков, форм например, анкет, квитанций и т.п. Бланки хранятся в системе в виде, недоступном для просмотра ни пользователям, ни администраторам Системы. См. также: Технологии, Элемент технологий
Вердикт	Атрибут события, содержащий заключение о наличии или отсутствии нарушений в анализируемом событии. В сочетании с атрибутом Транспортный режим определяет возможность дальнейшей транспортировки события. См. также: Транспортный режим, Состояние доставки, Атрибуты события, Событие

Термин	Определение
Версия конфигурации	Фиксированное состояние конфигурации, используемое для контроля изменений в настройках анализа событий. Версия конфигурации фиксируется в момент её загрузки на хост, и может быть активной (используемой в настоящий момент), редактируемой (последняя версия с текущими изменениями) или сохраненной (имеющей изменения и доступной для редактирования пользователями). См. также: Конфигурация
Виджет	Элемент интерфейса в виде обособленной области, выводящий заданную статистическую информацию о нарушениях и нарушителях. См. также: Консоль управления, Нарушение, Нарушитель
Вложение	Файл, приложенный к перехваченному событию, любой степени вложенности. См. также: Событие
Выгрузки из БД	Технология поиска цитат из базы данных. Выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и т.п. См. также: Технологии
Графические объекты	Технология поиска изображений (например, изображений паспорта или банковской карты) в тексте и вложениях перехваченных событий. См. также: Технологии, Событие, Объект защиты
Группа персон и компьютеров	Группа, объединяющая информацию о компьютерах организации, сотрудниках организации, а также внешних контактах. Группы делятся на Группы AD (импортированные из Active Directory) и Группы TM (созданные средствами IW TM). См. также: Персона, Компьютер, Контакт
Заголовки	Вспомогательные данные, размещаемые в начале блока хранимых или передаваемых данных. Используются для формирования в Системе сущности события и определения значений атрибутов этого события. См. также: Событие, Атрибуты события
Задача	См. Задача сканирования
Задача сканирования	Операция (единоразовая или повторяющаяся по расписанию) проверки целевых мест хранения информации (хранилище Microsoft SharePoint 2007/2010/2013, локальные диски рабочих станций, разделяемые сетевые ресурсы) на предмет наличия в них файлов, содержащих элементы технологий. См. также: Краулер, Сканер, Элемент технологий
Защищаемые данные	Набор объектов защиты, их каталогов и файловых форматов, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику защиты данных, в которой этот набор определен. См. также: Объект защиты, Файловый формат, Политика защиты данных
Значимость термина	Степень того, насколько данный термин характеризует категорию; целое число в диапазоне от 1 до 10. Если термин имеет высокую значимость, то при его обнаружении в объекте существует большая вероятность того, что данный объект может быть отнесен к категории, содержащей данный термин. См. также: Термин
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с системой.

Термин	Определение
Канал перехвата данных	Среда перехвата данных, состоящая из технических средств перехвата данных, средств программного обеспечения и протоколов передачи данных. В системе поддерживаются следующие каналы перехвата данных: электронная почта (SMTP, IMAP и POP3), веб (HTTP, HTTPS), сервисы мгновенных сообщений (Jabber, ICQ и Skype), теневые копии файлов, события подключения/отключения рабочих станций, задания на печать.
Категории и термины	Технология, выявляющая в тексте события наличие слов и выражений из базы терминов и относящая событие к категории, к которой принадлежат найденные термины. Ранее: Классификатор, БКФ. См. также: Событие, Термин, Категория, Технологии, Объект защиты
Категория	Именованная группа терминов, характеризующих определенную тематику. Если Система обнаруживает какой-либо из терминов категории в тексте перехваченного события, то она относит событие к этой категории. См. также: Термин
Компьютер	В терминах Системы под компьютером подразумевается контролируемая рабочая станция или мобильное устройство или терминальное устройство. См. также: Рабочая станция, Мобильное устройство, Терминальное устройство
Консоль управления	Графический интерфейс пользователя. Предназначен для управления системой (администрирование Системы, настройка конфигурации, анализ событий и т. п.).
Контекст события	Внутреннее представление перехваченного события в Системе. XML данные (атрибуты, текст), извлеченные из события и его вложений. После обработки с помощью технологий к контексту добавляются результаты анализа и информация о решении по событию. См. также: Событие, Технологии, Решение
Контролируемые персоны	Набор персон, групп персон и статусов персон, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику контоля персон, в которой этот набор определен. См. также: Персоны, Группа персон, Статус персоны, Политика контроля персон
Конфигурация	Набор настроек, необходимых для проверки событий а также для мониторинга и анализа данных. См. также: Событие, Технологии, Списки, Политика
Корпоративная политика безопасности	Принятая в компании совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, регламентирующих все вопросы обеспечения безопасности информации
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимое количество пользователей, используемые технологии и перехватчики и т.п. Также см.: Технологии, Перехватчики
Маска	Шаблон поиска — метод описания поискового запроса с использованием метасимволов. Маски используют для поиска файлов и папок
Мобильное устройство	Тип компьютера: смартфон или планшетный компьютер с установленной ОС семейства Android, Windows Phone или iOS. См. также: Компьютер
Монитор	См. Перехватчик
Морфология	Параметр термина: при использовании морфологии поиск по тексту будет осуществляться с учетом всех форм этого термина. См. также: Термин

Термин	Определение
Нарушение	Значение атрибута «Решение», означающее, что зарегистрировано нарушение корпоративной политики безопасности. См. также: Решение, Корпоративная политика безопасности
Нормальный транспортный режим	Режим, в котором выполняется анализ и фильтрация проходящего трафика. В этом режиме возможна блокировка запрещенного Системой трафика. См. также: Транспортный режим, "В разрыв"
Область видимости	Способ разделения перехваченных событий для ограничения доступа к ним пользователей консоли управления. События, удовлетворяющие критериям вхождения в какую-либо область видимости, будут видны только тем пользователям, которые имеют доступ к этой области видимости (при условии, что пользователь имеет привилегии на просмотр и/или работу с объектами). См. также: Событие, Привилегия
Объект защиты	Набор элементов технологий, обнаружение которых в событии позволяет отнести это событие к определенному типу бизнес-документов (каталогу объектов защиты). Объекты защиты используются при определении политик защиты данных. См. также: Элемент технологий, Политика защиты данных.
Основание вердикта	Атрибут события, описывающий причину, по которой событию был присвоен вердикт. См. также: Атрибуты события, Вердикт
Отчет	Выборка, обеспечивающая наглядное отображение статистических данных о событиях. См. также: Консоль управления, Событие
Офицер безопасности	Основной пользователь Консоли управления. Также - предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в системе, за исключением административных. См. также: Консоль управления, Пользователь, Роль пользователя, Привилегия, Администратор
Перехват данных	Процесс получения, разбора, рубрикации и преобразования данных (или их копии) в контекст. Осуществляется перехват данных, передаваемых по протоколам SMTP, IMAP, POP3, HTTP, HTTPS, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. См. также: Перехватчик, Контекст события
Периметр	Контейнер, содержащий элементы инфраструктуры компании (персоны, компьютеры, домен и прочие) и контактные данные. Используется для того, чтобы логически разделить организацию на структурные элементы и следить за трафиком каждого из таких элементов. См. также: Группа персон и компьютеров
Персона	Учетная запись сотрудника организации или внешнего контакта, содержащаяся в справочнике Системы и позволяющая обрабатывать данные, принадлежащие этой учетной записи, как единое целое, а также отображать события, относящиеся к ней, в удобном для пользователя виде. См. также: Группа персон и компьютеров
Политика	Совокупность правил, в соответствии с которыми проводится анализ и обработка событий. См. также: Политика, Активная политика, Правило
Политика контроля персон	Политика для оперативного добавления правил контроля персон, групп персон или персон с указанным статусом. См. также: Политика, Правило контроля персон, Персона, Статус персоны
Пользователь	Пользователь системы Traffic Monitor - администратор, офицер безопасности и др. См. также: Администратор, Офицер безопасности, Персона

Термин	Определение
Пользователь Консоли управления	Пользователь, в задачи которого входит выполнение различных функций по управлению Системой. Каждому пользователю назначается роль в соответствии с требованиями корпоративной политики безопасности.
Порог встречаемости	Количество текстовых объектов, найденных в событии, достаточное для обнаружения объекта защиты, в котором определен данный порог встречаемости. См. также: Событие, Текстовые объекты, Объект защиты
Порог цитируемости	Процент эталонного документа, найденный в событии в виде цитат, достаточный для отнесения события к этому эталонному документу. См. также: Событие, Эталонный документ, Цитата
Правило	Сущность, определяющая действия Системы в ответ на те или иные действия персон с защищаемыми объектами. Правило состоит из набора условий, по которым ведется проверка событий, и действий, осуществляемых при выполнении или невыполнении заданных условий. См. также: Событие, Политика, Защищаемый объект, Правило контроля персон, Правило копирования, Правило передачи, Правило хранения
Правило контроля персон	Правило, назначающее атрибуты событию с указанным уровнем нарушения, и в котором среди отправителей или получателей есть персоны, указанные в политике, куда входит это правило. Позволяет переназначать статус персонам и отправлять уведомления. См. также: Правило, Атрибуты события, Персона, Уровень нарушения, Статус персоны, Уведомление, Политика контроля персон
Правило копирования	Правило, регулирующее копирование, печать и фотосъемку защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Правило передачи	Правило, регулирующее отправку и получение защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Правило хранения	Правило, регулирующее хранение защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных, Краулер
Привилегия	Сущность, определяющая возможность пользователя выполнять какое-либо действие (набор действий) при работе с системой
Прокси-сервер	Служба, позволяющая выполнять косвенные запросы к другим сетевым службам. Прокси передает все запросы программ абонента в сеть, и, получив ответ, отправляет его обратно абоненту.
Рабочая станция	Тип компьютера: десктоп или ноутбук с ОС семейства Windows, Linux или Mac. См. также: Компьютер
Режим копии	Один из транспортных режимов системы IW TM. В этом режиме реальный трафик не проходит через Систему. Анализу подвергается копия трафика. В данном режиме невозможна фильтрация трафика средствами Системы. См. также: Транспортный режим
Решение	Заключение офицера безопасности о том, является ли событие нарушением корпоративной политики безопасности. Может принимать значения «Решение не принято», «Нарушение» и «Нет нарушений». См. также: Офицер безопасности, Корпоративная политка безопасности, Событие, Атрибуты события, Нарушение, Политика, Вердикт

Термин	Определение
Роль пользователя	Совокупность привилегий, определяющих набор действий, которые пользователь может выполнять при работе с системой. См. также: Администратор, Офицер безопасности, Консоль управления, Привилегия
Сводка	Раздел Консоли управления, отображающий статистическую информацию по нарушениям и нарушителям на виджетах. См. также: Консоль управления, Виджет, Нарушение
Сигнатура файла	Целочисленная константа, используемая для однозначной идентификации файлов определенного типа
Сканер	Служба Краулера, выполняющая проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративной политики безопасности. См. также: Краулер, Корпоративная политика безопасности
Событие	Объекты перехвата трафика (SMTP-, IMAP-, POP3-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения), теневые копии файлов и задания на печать. Создаются Системой в результате обмена данных между сотрудниками организации и другими людьми, включая публикацию в общедоступных источниках, копирование на внешние устройства и печать.
Состояние доставки	Атрибут события, определяющий возможность доставки события получателям после анализа. Если доставка события была разрешена, то значение атрибута отражает состояние доставки (выполнена/не выполнена). См. также: Атрибуты события
Списки	Списки однотипных данных, создаваемые средствами консоли управления, для использования при составлении политик. См. также: Конфигурация, Политика
Справочники персон, рабочих станций и групп	Данные о пользователях, рабочих станциях, а также группах персон и рабочих станций, импортированные из Active Directory, а также созданные средствами консоли управления. Используются для удобства работы с информацией о событиях
Статус	Характеристика персон и компьютеров, позволяющая разделять их по группам для удобства анализа и отслеживания активности, а также отображать в сводке и в отчетах с особой цветовой индикацией. См. также: Персоны, Компьютеры, Сводка, Отчет
Стоп-слово	Цифры, буквы и слова, нахождение которых в ячейках не приводит к срабатыванию этих ячеек. Стоп-слова используются для исключения ложноположительных срабатываний.
Тег	Текстовая метка, дающая краткую характеристику событию. См. также: Атрибуты события
Текст события	Текстовая информация, извлечённая из тела события и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска. См. также: Событие, Тело события
Текстовые объекты	Технология, соотносящая данные из текста событий, с заданными шаблонами (например, с правилами формирования номеров банковских карт). См. также: Технологии, Событие, Элемент технологий, Шаблон текстового объекта
Теневая копия документа	Копия документа, отправленного на печать с контролируемого компьютера. См. также: InfoWatch Device Monitor

Термин	Определение
Теневая копия файла	Копия файла, записываемого на съемное устройство. Создается только при успешном завершении операции сохранения файла на съемное устройство. См. также: InfoWatch Device Monitor
Термин	Один из набора слов и словосочетаний, в совокупности определяющих предметную область. См. также: Категория
Технологии	Набор инструментов анализа, выполняющих поиск заданных элементов в контексте событий и добавляющие событию атрибуты, характеризующие это событие. См. также: Элемент технологий, Контекст события, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты
Транспортный режим	Атрибут события, определяющий степень контроля доставки событий получателям. В сочетании с атрибутом "Вердикт" определяет возможность дальнейшей транспортировки события. См. также: Событие, Атрибуты события, Вердикт, Режим копии, Нормальный транспортный режим, Состояние доставки
Уведомление	Сообщение, отправляемое в случае срабатывания политики на событии. Отправляется средствами Консоли управления для уведомления пользователей Консоли управления, сотрудников или третьих лиц. Содержит краткую информацию о перехваченных событиях и сопроводительное сообщение. См. также: Политика, Событие
Уровень нарушения	Атрибут события, с помощью цветовой метки указывающий на степень угрозы для корпоративной политики безопасности. См. также: Событие, Атрибуты события, Нарушение
Учет регистра	Параметр термина: при учете регистра в анализируемом тексте будет выполняться поиск только тех словоформ, в которых есть полное соответствие с заглавными и строчными буквами, заданными в термине. См. также: Термин
Цитата	Отрывок эталонного документа, найденный в тексте события. См. также: Эталонный документ
Цитируемость	Показатель того, насколько полно эталонный документ присутствует в тексте анализируемого документа. См. также: Эталонный документ, Цитата
Цифровой отпечаток	Способ хранения эталонного документа в базе данных в виде набора цитат. См. также: Эталонный документ, Цитата
Шаблон текстового объекта	Унифицированное описание всех возможных текстовых объектов с типичной структурой: номера паспортов, кредитных карт, телефонные номера, код медицинского диагноза и т.д. См. также: Текстовые объекты
Элемент технологий	Составляющая настройки технологий, входящих в состав Системы. Пример конфиденциальных данных. К элементам технологий относятся: категории и термины, эталонные документы, бланки, выгрузки, текстовые объекты и графические объекты. См. также: Технологии, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты, Объект защиты.
Эталонная контрольная сумма	В отличие от текущей контрольной суммы, фиксирует образцовое состояние файлов Системы. См. также: Контроль целостности

Термин	Определение
Эталонные документы	Технология поиска цитат из конфиденциальных документов: например, образцы текстов приказов, финансовых отчетов, договоров и др. Эталонные документы хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы. См. также: Технологии, Элемент технологий, Цифровой отпечаток, Цитата